PROCEEDING

2'IWCA'19

Second International Workshop on Cryptography and its Applications

18-19 June 2019, U.S.T.O-MB, ORAN. ALGERIA

University of Sciences and Technology of Oran - Mohamed Boudiaf
Faculty of Electrical Engineering/ (USTO-MB)

Our Sponsors & Supporters

Table of contents

4	45-52	Hana ALI-PACHA Naima HADJ-SAID Adda ALI-PACHA	Proposition of a New Vernam Chaotic Cipher	University of Science and Technology of Oran
5	53-59	Mohamed Issad Mohamed Anane Bachir Boudraa Ahmed Mohamed Bellemou Nadjia Anane	Efficient FPGA Implementation of ModularMultiplication and Exponentiation	Centre de Développement des Technologies Avancées-CDTA Ecole Supérieure d'Informatique-ESI USTHB Houari Boumediene, Bab Ezzouar, Alger Centre de Développement des Technologies Avancées-CDTA
6	60-64	Karima Chatouh	A Presentation of a Linear Code over : $\mathcal{A}_{q,3} = \mathbb{Z}_q[u_1, u_2, u_3] / \langle u_i^2 = 1, u_i u_j = u_j u_i \rangle$	*Mostefa Ben Boulaid* University, Batna 2. Batna
7	65-71	Lamiche Chaabane	An Improved Encryption Approach Based on Multi-chaotic Maps Applied to Digital Image	Mohamed Boudiaf university M'sila
8	72-77	Mohamed Issad Nadjia Anane Ahmed Mohamed Bellemou Bachir Boudraa	Secure Hybrid Crypto-system AES/RSA on FPGA for Data Communication	Centre de Développement des Technologies Avancées-CDTA USTHB Houari Boumediene, Bab Ezzouar, Alger
9	78-79	Nacer Ghadbane	On public key cryptosystem based on the word problem in a group	Mohamed Boudiaf university M'sila
10	80-85	Hichem BOUCHAKOUR ERRAHMANI Hind IKNI	A New Approach to Verifying and Sharing a Secret QR Code using Elliptic Curves	Djillali Liabes University Sidi Bel Abbes Belhadj Bouchaib Center-University Ain Temouchent,
11	86-99	*Abdelkader GHAZLI* *Adda ALI-PACHA* *Naima HADJ SAID* *Boubakeur Ghazli*	Security Enhancements of A5/1 Based Particle Swarm Optimization for Mobile Telecommunication Networks	Tahri Mohamed University of Bechar Université des Sciences et de la Technologie d'Oran Mohamed Boudiaf, USTO Tahri Mohamed University of Bechar
12	100-115	DJAMEL BELLAOUAR	Nonstandard notes on the ratio of two expressions formed by the product and the sum of certain multiplicative arithmetic functions	University of Guelma

31	221-224	Mahdjoubi Roumaissa	New Signature Algorithm Based on Concatenated Rank Codes	*University of Science and Technology Houari Boumedien* Algiers
		Sedat Akleylek		
		Kenza Guenda		
32	225-228	Rekkal kahina	Encrypting the TCM Encoder with Locally Rotated Constellations in Rayleigh Fading Channel	Tahri Mohammed University-Bechar
		Rekkal Sarah		university of Oran1 ahmed ben bella
		Abdesselam Bassou		Tahri Mohammed University-Bechar
33	229- 233	Amine Zellagui	Secure MD4 Hash Function Using Henon Map	University of Science and Technology of Oran
		Naima HADJ-SAID		
		Adda ALI-PACHA		
34	234-238	ALI CHERIF Khalfallah	Using of Multi Chaotic System for Implementing a Good Cryptosystem	University of Science and Technology of Oran
		Naima HADJ-SAID		
		Adda ALI-PACHA		
35	239-249	Hadj Ahmed BOUARARA	Detection and Prevention of Suicidal Self-harm Behavior in Twitter	*Molay Tahar university of saida algeria*
36	250-255	BAIDAR Lotfi	PSO Variants for Localization Challenge in Wireless Sensor Network and Internet Of Thing	Ecole Superieure en Informatique, Sidi Bel Abbes, Algeria
		RAHMOUN Abdellatif		
		LORENZ Pascal		IUT of Colmar, University of Haute Alsace, Mulhouse ,France
		Miloud Mihoubi		Djillali Liabes University, Sidi Bel Abbes, Algeria
37	256-261	LAAJI EL Hassane	Two new Quantum Attack Algorithms against NTRU pke # KA NTRU # & # PA NTRU #.	Mohammed First University, Oujda, Morocco
		AZIZI Abdelmalek		
		AZZOUAK Siham		Sidi Mahammed Ben Abdellah University, Fes, Morocco
38	262-269	Hebbache Zineb	Study On Skew Codes over The ring Zq + uZq	Univesity of Science and Technology Houari Boumedien, Algiers, Algeria
		Guenda Kenza		

WELCOME MESSAGE FROM THE CONFERENCE CHAIR

Madam the Rector of the University

Dean of the Faculty of Electrical Engineering,

Honorable guests,

Dear Students

Dear Colleagues,

Ladies and Gentlemen,

Good Moring to you all and, welcome to our city Oran, where we have the pleasure and the honor to welcome you for this second international workshop on cryptography and its applications (2'IWCA 2019), organized by the University of Sciences and of Oran-Mohamed Boudiaf Technology in conjunction with the LACOSI Laboratory (Lab. of Coding and Security of Information) of USTO-MB. This workshop, which follows the first one organized in April 2016 at the USTO-MB Oran.

The main objective of this workshop is to provide an update on the latest advances in cryptography and computer security: methods, technologies and applications: Domain requiring the perfect mastery of mathematical, computer and electronic tools.

In this context, the USTO-MB has seen the establishment since October 2013 of an Academic Master "Cryptography and Data Security" approved by the Ministry and domiciled in the Department of Electronics where we have formed promotions, before the Ministry's harmonization reform of the Masters. In addition, there is creation of a doctoral training entitled "Cryptography and Data Security" approved by our tutelage since June 2016, until today.

The concept of computer security and the Internet has constantly changed its face and dimension as well as the evolution of technologies. With the advent of the Internet, computer networks and the use of satellite links, the new industrial revolution in computing and telecommunications has led to the storage and to the transmission of large amounts of confidential data and a growing concern for to protect access. Therefore, encryption is necessary so that the data is unintelligible except to the intended audience.

The problem is how to implement security measures and solutions effectively to really protect information systems. Security strategies result in the proposal and implementation of a security policy.

Unfortunately, today we realize that despite all the security measures and strategies that can be implemented, information systems are nevertheless vulnerable to certain targeted attacks or intrusions. This is why for some years now, security experts have been talking about, on the one hand, more and more of a new concept namely intrusion detection, and on the other hand about the design of post-quantum cryptosystems.

That is why this event is aimed at the national university research community, first and foremost, the users, who participate in the developments of data security and their implementation.
In addition, it is a question of establishing contacts between university researchers and those responsible for its services in such a way as to launch an effective cooperation between the two parties, in the interest of the development of the country.

Major goals:

A. Organize tutorials for new PhD students;
B. Encourage PhD students to present the results of their work
C. Promotion of exchanges of knowledge and experience between national and international researchers;
D. Initiating national and international cooperation between academia and industry in the field of telecommunications security (eg Smart Card and RFID).
E. Reiterate reflection on the creation of an Algerian Association for Cryptography.
F. The initiation of lines of thought that will be the subject of future meetings organized by the Faculty of Electrical Engineering of the USTO-MB.

However, for this workshop, we selected 6 themes:

• Cryptographics standards and applications
• Cryptographic algorithms, their FPGA design and implementation
• RFID - security and cryptography aspects, etc.
• Chaos Generation, Characterization and Synchronization
• Biometry
• Mathematics tools for cryptography and for coding

For the success of this workshop, there are indeed many people to thank. The scientific committee did an outstanding job and organizing a very high quality program. The organizing committee is very grateful to scientific and technical supplier enterprise, for their generous sponsoring and support.

I am blessed with the presence of our distinguished keynote speakers; who are ones of the prominent Professors in the world in their respective areas, or even just the founders of their respective research areas. Their participation and contribution are deeply appreciated.

I hope you will have a rewarding experience and enjoyable time at the conference

Conference chair

Prof. ADDA ALI PACHA

University of Sciences and Technology of Oran - Mohamed Boudiaf
Faculty of Electrical Engineering/ (USTO-MB)

Department of Electronics

LACOSI. Lab: Laboratory of **Co**ding and **Se**curity of **I**nformation

2'IWCA'19

Second International Workshop on Cryptography and its Applications 18-19 June 2019, U.S.T.O-MB, ORAN. ALGERIA

https://www.univ-usto.dz/2IWCA19/
Tel/fax: (+213/0) 41 62 71 60

ANNOUNCEMENT AND CALL FOR PAPERS

DEAR COLLEAGUES,

We are pleased to announce that the Second International Workshop on Cryptography and its Applications
(2'IWCA'19) will be held in Oran, Algeria on June 18-19, 2019 with the collaboration of the University of Sciences and Technology of Oran – (USTO-MB), ALGERIA, and Ondokuz Mayıs University (OMU), Samsun, TURKEY.
The aim of this workshop is to bring together researchers and experts to provide a sharing platform for the latest advances in cryptography and computer security: methods, technologies and applications. This workshop aims to establish contacts between universities, companies, institutions, agencies and entrepreneurs in such a way to launch effective cooperation between the two parties in the interest of the development of local and international industry. Official language of the workshop is English.

MAJOR OBJECTIVES

A. Organize tutorials for new PhD students;
B. Encourage PhD students to present the results of their work
C. Promoting exchanges of knowledge and experience between national and international researchers;
D. Initiating national and international cooperation between academia and industry in the field of telecommunications security (e.g. Smart Card and RFID).

Honorary President of the conference: The Rector of the USTO-MB, Prof. Benharrats Nacéra

Conference Chairs: Prof. Adda Ali-Pacha and Prof. Sedat Akleylek

Topics within the scope of the conference include the following areas, but not limited to:

- *Cryptographics standards and applications*
- *Cryptanalysis*
- *Cryptographic algorithms, their design and implementation FPGA*
- *Number theory, elliptic curves, lattices and coding theory*
- *Cryptography and legislation*
- *Quantum and Post-Quantum cryptography*
- *Privacy enhancing technologies*
- *Provable security •*
- *Blockchain*
- *RFID security and cryptography aspects, etc.*
- *IoT security*
- *Cryptographic software*
- *Chaos Generation, Characterization and Synchronization*
- *Chaos-based Crypto and Crypto Compression Systems*
- *Chaos based Steganography*
- *Chaos-based Watermarking*
- *Chaos-based Crypto-Biometric Schemes*
- *Biometry*
- Steganography
- Cloud Computing Security
- *Cyber Security*
- *Watermarking*
- *Malware and Viruses*
- *Wireless Network Security (Internet, WSNs, UMTS, WiFi, WiMAX, WiMedia and others)*
- *Physical layer security*

STEERING COMMITTEE

1. Berrached Nasr-Eddine
2. Alshaqaqi Bilal
3. Boumehed Meriem
4. Daoud Amine
5. Ghazli Abdelkader
6. Henkouche Damel
7. Hamdaoui Sid Ahmed
8. Lakhdari Fethi
9. Abdeladim Mustapha
10. Merah Lahcen
11. Rahmani Bouabdallah
12. Chouraki Samira
13. Rimani Rachid
14. Belalia Djillali
15. Soudani Said

SCIENTIFIC COMMITTEE : **HONORARY CHAIRMAN: *PR. BACHIR GHALEM.***

Dean of the Faculty of Electrical Engineering

1. Abdelkader NECER, Limoges University, France
2. Abdelmalek AZIZI, Mohamed Premier, University, Oujda, Marocco
3. Ahmet Sınak, Konya Necmettin Erbakan University, Turkey
4. Akram M. Zeki, International Islamic University Malaysia
5. Amroune Abdelaziz, Univ. M'sila, Algeria
6. Arab ALI CHERIF, Univ. Paris 8, France
7. Asma Adnane, Loughborough University, UK
8. Aydin Secer, Yildiz Technical Univ. Turkey
9. Baghdadi Azzedine, Univ. Paris 13
7. Barbot Jean Pierre ENSEA -Cergy Pointoise
8. Baris Bulent Kirlar, Suleyman Demirel University, Turkey
9. Bayram Mustafa, Univ-Gelisim, Turkey
10. Benmohamed Mohamed, Univ. Constantine
11. Benslama Malek, Univ. Constantine, Algeria
12. Besik Dundua, Tbilisi State University, Georgia
13. Boufeldja ALLAILOU, ESACH-Alger
14. Bourennane Mohamed, University of Stockholm

15. Bouridane Ahmed, Northumbria University, UK
16. Camal Tanougast, Univ Lorraine, France
17. Christophe Letellier, Univ. de Rouen
18. Damien Sauveron, University of Limoges
19. Daniel ROVIRAS, CNAM Paris
20. Feham Mohamed, Univ. Tlemcen, Algeria
21. Feraoun Mohamed Kamel Univ. Sidi Belabes
22. Ferruh Ozbudak, Middle East Technical University, Ankara, Turkey
20. Ghanes Malek, Univ-Nantes
21. Ghoualmi-Zine Nacira, Univ. Annaba
22. Guenda Kenza, USTHB, Algeria
23. Guillot Philippe, Univ. Paris 8
24. Juan Antonio Lopez Ramos, Univ. Almeria, espagn
25. Hadj Said Naima, USTO Oran, Algeria
26. Hamadouche M'hamed, Univ. Boumerdes
27. Hamri Nasreddine, Univ. Mila
28. Hmaied Shaiek, , CNAM Paris
29. Ion Tutanescu, Pitesti University, Romania
30. Larger Laurent, Univ-fcomte, France
31. Loukil Abdelhamid, USTO-Oran, Algeria
32. Lozi René Univ-Nice
33. Martin Liess, RheinMain University of Applied Sciences, Germany
34. Meziane Abdelkrim CERIST Alger
35. M'hamed Abdallah Télécom SudParis France
36. Mikheil Rukhaia, Tbilisi State University, Georgia
37. Mohamad Afendee Mohamed, (Universiti Sultan , Zainal Abidin, , MALAYSIA
38. . Mohamed Saied Emam, Darmstadt University of Technology, Germany
39. Mokrane Abdellah, Univ. Paris 8
40. Muhammet Kurulay, , Yildiz Technical Univ. Turkey
41. Muharrem Tolga Sakalli, Trakya University, Turkey
42. Mustafa bin Mamat, Univ Sultan Zainal Abidin, 21300 K Terengganu, MALAYSIA
43. Murat Cenk, Middle East Technical University, Turkey
44. Naït-Abdesselam Farid, Paris Descartes University
45. Narasimha Shashidhar, Sam Houston State, University, USA
46. Nguyen Ngoc Cuong, Academy of Cryptography Technic of Viet Nam.
47. Nitaj Abdelrahman, Univ. Caen
48. Noui Lemnaouar Univ. Batna, Algeria
49. Oguz Yayla, Hacettepe University, Turkey
50. Ouslim Mohamed, USTO- Oran, Algeria
51. Ouslimani Achour, ENSEA -Cergy Pointoise
52. Pascal LORENZ, Univ. Mulhouse
53. Puech William, Univ. Montpellier
54. Rachid Nourine, INTITIC, Oran, Algeria
55. Safwan El Assad, Univ-Nantes
56. Sedat Akleylek, Ondokuz Mayıs University, Samsun, turkey
57. Serhrouchni Ahmed, Telecom-ParisTech, France
58. Snouci AEK, ESACH-Alger
59. Zulfukar Saygi, TOBB ETU, Turkey
60. Zouagui Tarek, USTO-Oran, Algeria

INSTRUCTIONS TO AUTHORS

The organizing committee proposes to provide an update on all the topics related to this scientific conference in plenary, oral and poster (poster). The two-day program will be finalized on the basis of the replies of the invited experts. The content of any submissions should be original and must not be submitted simultaneously for consideration towards publication in any other conference or journal. Reuse of material previously published by the authors is possible under the conditions that the authors fully disclose/cite the references and any similarity will not exceed 30% of the current submission.

Authors interested in this conference are invited to submit their proposals to full papers in PDF or Word format in English, mentioning it electronically title of the paper, affiliations and email address. Papers should not exceed 8 pages and must be prepared in accordance with IEEE conference format. Depending on the IEEE style downloadable from the site: http://www.ieee.org//conferences_events/conferences/publishing/templates.html

Selected papers will be published in the International Journal of Organizational and Collective Intelligence (IJOCI), or in the Malaysian Journal of Computing and Applied Mathematics (MyJCAM, https://myfik.net/myjcam/index.php/myjcam) or in the Algerian Journal of Research and Technology (AJRT).

The submission site is not open at: https://easychair.org/conferences/?conf=2iwca19

Submission deadlines:

05/15/2019 : Submission of the complete paper
05/20/2019 : Notification of acceptance of the paper
05/27/2019 : Camera ready, final version of the paper

Registration fees (The fee covers accommodation, lunch, coffee breaks and social event**)**

Author participant: 5000 DA
Student: 3000 DA
Foreigners: 100 Euros
Other: 10000 DA

CONTACTS

For further information contact:

Secretariat of the Workshop 2'IWCA'19
Department of Electronics, Faculty of Electrical Engineering, USTO-MB
BP 1505 EL M'Naouer Oran (31000) Algeria
Mob. : +213 664811717 // +90 362 3121919-1099
E. mail: iwca2019@univ-usto.dz and ic2016ca@gmail.com
Web site: https://www.univ-usto.dz/2IWCA19/

****

Registration and information form

I intend to present a paper to 2IWCA'19

Oral Session	Poster Session
I intend to participate with an exhibition at 2IWC A'19	

Check the relevant boxes

Last and First Name : ……
Position:……
Institution or Company:…….....
Affiliation:……
Address:…….

Tel:…….
Fax:……
E-mail:……

article

Theme:

Title of the paper: …….....

Authors:……

and return it to the e-mail address: ic2016ca@gmail.com

Université des Sciences et de la Technologie d'Oran - Mohamed BOUDIAF

International Workshop on Cryptography and its Applications – 2'IWCA'19 -

18 & 19 Juin 2019, U.S.T.O-MB, ORAN-ALGERIE

https://www.univ-usto.dz/2IWCA19/

Tél : +213/ 664811717

PROGRAMME

Tuesday, June 18th

8:00-9:15	**Registration**
9:15-9:45	**Opening Remarks**

Plenary Session 1

Co-Chairs: M. Benslama / N. Berrached

9:45-10:25	Ahmed Bouridane	Artificial Intelligence: Risks and Benefits

Plenary Session 2

Co-Chairs: L. Noui / N. Rahmani

10:25-11:05	A. M'HAMED (Télecom / Télécom Sud Paris)	Cryptographic Tools in Cloud Storage

11:05-11:30	**Coffee Break** **Souvenir Pictures**

Oral Session 1 Co-Chairs: M. Snouci / A. Ouamri		
11:30-11:45	Mohamed SAOUDI, ESACH/ Algiers	"Efficient Hardware Implementation of Elliptic Curve Diffie-Hellman Key Exchange Protocol",
11:45-12:00	M. Issad, CDTA	"Efficient FPGA Implementation of Modular Multiplication and Exponentiation",
12:00-12:15	M. Issad, CDTA	"Secure Hybrid Crypto-system AES/RSA on FPGA for Data Communication"
12:15-12:30	Omar Hocine BENHADDAD, ESACH/ Algiers	"Hardware Acceleration of AES Cryptographic Algorithm for IPsec",
12:30-12:45	Ali HADOUDA, Univ. of Oran1	"A New Efficient Approach Based on Chaotic Map for Image Encryption"
12:45-13:00	Mahdjoubi Roumaissa, USTHB, Alger	"New Signature Algorithm Based on Concatenated Rank Codes",

13:05-14:15	**Lunch**

Plenary Session 3 Co-Chairs: M. Keche / F. Khelfi		
14:20-15:00	Bilal EL ALAMY	Blockchain for Social and Economic Empowerment

Oral Session 2 Co-Chairs: R. Nourine / A. Baghdadi		
15:00-15:15	Sarah Moussaoui, ECRMT/Algiers	"Implementation and statistical tests of a blockcipher algorithm MISTY1",
15:15-15:30	Lamiche Chaabane, univ. M'sila	"An Improved Encryption Approach Based on Multi-chaotic Maps Applied to Digital Image"

15:30-15:45	Hichem BOUCHAKOUR Univ., Sidi Bel Abbes	"A New Approach to Verifying and Sharing a Secret QR Code using Elliptic Curves"
15:45-16:00	Oussama Nouir Univ. of Batna1	"A novel image encryption approach using polar decomposition and orthogonal matrices",
16:00-16:15	Khaled Hamouid, Univ. Batna,	"Anonymous communication in IoT based on verifiable encryption",

16:15-16:45	**Coffee Break**

Poster Session 1 Co-Chairs: M. Ould Mamar / M. Ouslim	
16:15-16:45	**Poster Session 1**

Oral Session 3 Co-Chairs: A. Bouridane / M. Djaa		
16:45-17:00	DJAMEL BELLAOUAR, Univ. of Guelma	"Nonstandard notes on the ratio of two expressions formed by the product and the sum of certain multiplicative arithmetic functions"
17:00-17:15	Noureddine Chikouche, Univ. M'sila	"Privacy Analysis of a New Authentication Protocol for Internet of Things"
17:15-17:30	EL Hassane LAAJI, *Mohamed First University, Oujda, Morocco*	*"Two new Quantum Attack Algorithms against NTRU pke # KA NTRU # & # PA NTRU #"*,
17:30-17:50	Mustapha MEFTAH, USTO-MB	"DNA Encryption Algorithm Based on Variable Coding Scheme",
17:50-18:05	Murat Demircioglu, METU Univ. Ankara, Turkey	*"Efficient GeMSS Based Ring Signature Scheme"*,
18:05-18:20	Ahmet Sınak, *Univ. Paris VIII, France; Necmettin Erbakan University, Turkey*	*"Three-Weight Minimal Linear Codes and Their Applications"*,

---

Wednesday, June 19th

Plenary Session 4 Co-Chairs: A. Bouyakoub / B. ALLAILOU		
8:45-9:25	Philippe GUILLOT (Univ. Paris 8)	Flatness and Submertivity in Discrete Time Dynamical Systems

Plenary Session 5 Co-Chairs: A. Snouci / K. Ferouan		
9:25-9:55	Mohamed Bourennane (Stockholm University)	QUANTUM SECURE COMMUNICATION

9:55-10:25	**Coffee Break**

Poster Session 2 Co-Chairs: B. Kechar / B. Al Alamy	
9:55-10:25	Poster Session 2

Oral Session 4 Co-Chairs: K. Guenda / A. M'hamed		
10:25-10:40	Ghalem kamel Ghanem, USTO-MB	"Recognition of individuals from iris images using fusion methods and support vector Machine",
10:40-10:55	A. GHAZLI, Univ. of Bechar	"Security Enhancements of A5/1 Based Particle Swarm Optimization for Mobile Telecommunication Networks"
10:55-11:05	Ahmed Yassine Boumedine, USTO-MB	"Face Identification using Kinect Depth-Maps under One Sample per Person Scenario",
11:05-11:20	M.Amine BOUDOUAIA, USTO-MB	"A Clustering algorithm for distributing certificates in OLSR protocol",
11:20-11:35	Sabri Ahmed, Univ. USTO	"Chaotic Encryption for Fingerprint Images",

11:35-12:00	R. RIMANI , USTO-MB	"Image encryption by AES algorithm based on chaos-Permutation",

Plenary Session 6 Co-Chairs: P. Guillot / M. Bourennane		
12:00-12:40	Azeddine Beghdadi (Univ. Paris 13)	Quality-driven Framework an Models for Effective Public Security and Multimedia security

Cloture Session Co-Chairs: A. Ali-Pacha / A. Beghdadi	
12:40-13:30	**Cloture and recommendation**

13:30-14:30	**Lunch**

Poster Session 1		

Tuesday, June 18th

16:15-16:45	**Oualid Benamara ,** *USTHB, Institute of Mathematics, Algeiers*	***Introduction to STARKs: Scalable, transparent, and post-quantum secure computational integrity***
	Chahira Rouifed, *University of Tizi-Ouzou- Algeria*	***Modeling and non-linear dynamic analysis of the chaotic Colpitts oscillator up to 1 GHz***
	Karima. Chatouh, *University, Batna 2,*	***A Presentation of a Linear Code over:*** $\mathcal{A}_{q,3} = \mathbb{Z}_q[u_1, u_2, u_3] / \langle u_i^2 = 1, u_i u_j = u_j u_i \rangle$ **„**
	Nacer Ghadbane, *University M'sila,*	***On public key cryptosystem based on the word problem in a group***
	Bilal SAOUD, *University of Bouira*	***Community structure in complex networks based on Tabu Search",***
	Ahlem Melakhessou, *University Batna2, DZ*	***" Double Skew (1+u) – Constacyclic codes over*** $\mathbb{Z}_4(\mathbb{Z}_4 + u\mathbb{Z}_4)$ **„,**
	Karima Djebaili, *University of Ouragla, Algeria*	***"A Different Encryption System Based on the Integer Factorization Problem",***
	Reguia Lamia Bouzara, *USTHB, Alger,*	***Lifted Codes over Finite Chain Rings",***
	Rekkal kahina, *University, Bechar, Algeria*	***"Encrypting the TCM Encoder with Locally Rotated Constellations in Rayleigh Fading Channel",***
	Hebbache Zine, *University of USTHB, Alger, Algeria*	***"Study On Skew Codes over The ring Zq + uZq",***
	Salah Salim Belaifa, *Djezzy Telecom Algeria*	***"Authentication, Cyphering & Security in Modern Mobile Network",***

Poster Session 2

Wednesday, June 19th

9:55-10:25	**Noureddine Chikouche,** *Mohamed Boudiaf University M'sila, Algeria*	***"SIMULATION OF ATTACKS ON AUTHENTICATION PROTOCOLS FOR NEAR FIELD COMMUNICATIONS"***
	Abdelkader Bouguessa , *University - USTO-MB, Algeria*	***New Technique of styganography based on the Theory of Chaos : Survey",***
	Hana ALI PACHA, *University - USTO-MB, Algeria*	***Proposition of a New Vernam Chaotic Cipher***
	Asmaa Aouat, *University of Oran1 Ahmed Benbella, Algeria*	***"Approach Management Application in Cloud Computing: Runtime vs Docker"***
	Amine Zellagui, *University - USTO-MB, Algeria*	***"Secure MD4 Hash Function Using Henon Map",–***
	Khalfallah ALI CHERIF, *University - USTO-MB, Algeria*	***"Using of Multi Chaotic System for Implementing a Good Cryptosystem",***
	Hadj Ahmed BOUARARA, *Moulay Tahar University , Saida, Algeria*	***"Detection and Prevention of Suicidal Self-harm Behavior in Twitter",***
	L. BAIDAR,' *Ecole Supérieure en Informatique ; Sidi Bel Abbes, Algeria*	***"PSO Variants for Localization Challenge in Wireless Sensor Network and Internet Of Thing",***
	Farah Bahmed,' *Ahmed Zabana University Centre, Relizane,, Algeria*	***"Hand Biometry: A Review",***

Plenary Speakers

Ahmed Bouridane

Ahmed Bouridane received an “Ingenieur d’Etat” degree in electronics from “Ecole Nationale Polytechnique” of Algiers (ENPA), Algeria, in 1982, an M.Phil. degree in electrical engineering (VLSI design for signal processing) from the University of Newcastle-Upon-Tyne, U.K., in 1988, and an Ph.D. degree in electrical engineering (computer vision) from the University of Nottingham, U.K., in 1992. From 1992 to 1994, he worked as a Research Developer in telesurveillance and access control applications. In 1994, he joined Queen’s University Belfast, Belfast, U.K., initially as Lecturer in computer architecture and image processing and later on he was promoted to Reader in Computer Science. He is now a full Professor in Image Engineering and Security and leads the Computational Intelligence and Visual Computing Group at Northumbria University at Newcastle (UK), and his research interests are in imaging for forensics and security, biometrics, homeland security, image/video watermarking, medical engineering, cryptography and mobile and visual computing. He has authored and co-authored more than 350 publications and two research books on imaging for forensics and security; and Biometric Security and privacy.
Prof. Bouridane is a Senior Member of IEEE.

Title : Artificial Intelligence: Risks and Benefits

Summary: Artificial Intelligence (AI) refers to the ability of a computer program/machine to think and learn like a human. AI applications already pervade many industries, bringing potential benefits that have been predicted to massively increase economic growth rate in a number of developed economies. However, the introduction of such innovative technology also brings new challenges. This seminar identifies some of the emerging risk issues around the growing implementation of AI and examines current and possible future implications of so-called "strong" AI, outlining potential benefits and areas of concern and their potential impact of AI in the security and defence industry.

For example, in security and defence applications, AI-powered software and machine (robots) can dramatically alter the digital security threat landscape. On one hand, it could help to reduce cyber risk by better detecting attacks, but on the other hand it could increase if malicious hackers are able to take control. AI could enable more serious incidents to occur by lowering the cost of devising cyber-attacks and enabling more targeted incidents. The same programming error or hacker attack could be replicated on numerous machines. For example, one machine could repeat the same erroneous activity several times, leading to an unforeseen accumulation of losses. It is already estimated that a major global cyber-attack has the potential to trigger massive losses. In addition, AI could also enable autonomous vehicles, such as drones, to be utilised as weapons. Such threats are often underestimated.

Existing AI applications are built around so-called "weak" AI agents, which exhibit cognitive abilities in specific areas, such as driving a car, solving a puzzle or recommending products/actions. With the first tangible benefits of "weak" AI applications already being deployed across many industries, expectations for AI technology are rising and more development investments are being allocated in order to anticipate the benefits of more human-like or "strong" AI in future. Its introduction especially with the current Deep Neural Network technology will most likely be unprecedentedly disruptive to current business models.

This seminar will first define and describe the concept of AI and a history of its development given. The operation of an AI system will then be given followed by a discussion of the dangers and benefits of the technology in light of the recent advances including the concept of Deep learning technology.

Azeddine Beghdadi

L2TI, Institut Galilée, Université Paris 13, Sorbonne Paris Cité

Dr. Azeddine BEGHDADI is Full Professor at the University of Paris 13 (Institut Galilée) Sorbonne Paris Cite since 2000. He is the founding member of the Laboratory of Information Processing and Transmission (L2TI laboratory) and was its director from 2010 to 2016. He started his education at ENSEP (Oran-Algeria) and Physics Institute at University Oran Es-Senia. He received Maitrise in Physics and Diplôme d'Etudes Approfondies in Optics and Signal Processing from University Orsay-Paris XI (Equivalent : Masters of Sciences) in June 1982 and June 1983 respectively and the PhD in Physics (Specialism : Optics and Signal Processing) from University Paris 6 in June 1986.

He published over than 280 international refereed scientific papers. His research interests include image quality enhancement and assessment, image and video compression, bio-inspired models for image analysis and processing, and physics-based image analysis. Dr. Beghdadi is the founder and Steering Committee Chair of the European Workshop on Visual Information Processing (EUVIP). Dr Beghdadi is associate editor of "Signal processing : Image Communication", Journal, Elsevier, European journal on image and video processing, Springer Verlag, Journal of Electronic Imaging, SPIE Digital Library, and Mathematical Problems in Engineering, Journal, Hindawi. He served as conference chair and technical chair of many IEEE conferences. He is a member of EURASIP and IEEE-MMTC and a senior member of IEEE.

Title : Quality-driven Framework an Models for Effective Public Security and Multimedia security

Summary

Public security and data protection are among the top research priorities of many governments. Securing sensitive data and monitoring systems are more and more demanding in terms of quality, reliability and flexibility especially those dedicated to public security and particularly video surveillance based systems. This talk aims to present some challenging issues related to visual data protection and video-surveillance. The importance of taking into account the perceptual quality of the acquired visual information, through a biologically-inspired framework, is demonstrated through some real-life scenarios. Here we mainly focus and two applications: visual data watermarking and video-surveillance. I will discuss some common distortions and artefacts that may affect the quality of the acquired signal and therefore the performance of data protection and the video-surveillance systems. Some results on how to mitigate theses artifacts introduced by environment and system limitations will be also presented. Few preliminary results will be presented and discussed in the light of recent advances and current trends in the field of visual information processing.

Mohamed Bourennane

Mohamed Bourennane, Full Professor, Head of Quantum Information and Quantum Optics Group, Physics department, Stockholm University, Sweden, Member of the Royal Swedish Academy of Sciences.

He has obtained his Ph.D. at Royal Institute of Technology, Stockholm, Sweden.

He was a research associate at Physics Department, Ludwig Maximilians University, Munich, and Max Planck Institute for Quantum Optics, Garching, Germany.

He has obtained the junior and senior Fellow from the Swedish Research Council (VR). He is holder of several research grants from Knut and Alice Wallenberg foundation, VR, and EU.

Title: QUANTUM SECURE COMMUNICATION

Abstract:

The banking, financial, and defense sectors crucially depend on communication through channels that cannot be intercepted by unauthorized people. Today, different types of sensitive information are sent within and between companies. All of these users employ cryptography to keep their data secret. Today's cryptographic protocols rely on RSA or so-called elliptical curves methods. Unfortunately, there is no guarantee that these methods will remain safe in the near future, especially having in mind potential growth of the computation power. Fortunately, quantum mechanics makes it possible to solve the key transfer problem in a new and proven safe manner. Unlike classical methods, it is the nature's laws that guarantee the security of quantum cryptography. In this talk, I will introduce and review quantum secure communication and the worldwide effort in quantum technologies.

Abdallah M'HAMED

Abdallah M'hamed est maître de conférences, HDR, à l'Institut Mines Télecom/Télécom Sud Paris. Après sa thèse de Doctorat en Contrôle des Systèmes qu'il a soutenue à l'Université de Technologie de Compiègne en 1990, il rejoint Telecom Sud Paris au poste d'enseignant chercheur en sûreté de fonctionnement et sécurité des réseaux. En 2011, il obtient son habilitation à diriger la recherche (HDR) en « Sciences pour l'ingénieur » à l'Université Pierre et Marie Curie et rejoint le groupe R3S du Laboratoire SAMOVAR (UMR 5157). Entre 2002 et 2007, il fût coordinateur de l'option « Sécurité des Réseaux et Systèmes » à Télécom Lille. Depuis 2011, il est responsable pédagogique du mastère spécialisé « Sécurité des Systèmes et Réseaux », à Telecom Suparis.
Entre 2000 et 2013, il fût membre du laboratoire HandiCom à Télécom Sud Paris où il a mené ses travaux de recherche sur la conception et l'implémentation d'une architecture d'authentification intégrant la sécurité, la confiance et la vie privée dans les environnements sensibles au contexte.
Ses activités d'enseignement sont principalement axées sur les services et mécanismes de sécurité, les systèmes cryptographiques et les modèles de contrôle d'accès.
Il a participé à l'organisation de séminaires dans le cadre de l'Institut pour la Maîtrise des Risques et du Forum ATENA.

Title : Cryptographic Tools in Cloud Storage

Summary :

In cloud environments, data protection is a major issue for building trust between the various players (customers and service providers). In order to solve security and privacy problems, we use cryptographic mechanisms adapted to the constraints and specificities of Cloud architectures. The objective is to present the panorama of cryptographic techniques dedicated to the protection of storage and data processing in cloud environments.

Résumé

Dans les environnements Cloud, la protection des données est un enjeu majeur pour instaurer la confiance entre les différents acteurs (clients et fournisseurs de service). Afin de résoudre les problèmes de sécurité et de vie privée, on a recours à des mécanismes cryptographiques adaptés aux contraintes et aux spécificités des architectures Cloud. L'objectif est de présenter le panorama des techniques cryptographiques dédiées à la protection du stockage et du traitement de données dans les environnements Cloud.

Philippe GUILLOT

CV :
- Études de mathématiques à l'Université Pierre et Marie Curie, et à l'Université de Rouen.
- Agrégation de Mathématiques en 1988.
- Doctorat en informatique, Université de Caen, "Fonctions courbes binaires et transformation de Möbius" en 1999.
- Ingénieur d'études en cryptologie à Thomson-CSF à partir de 1990.
- Chef du laboratoire de cryptologie de l'entreprise Thales jusqu'en 2001.
- De 2001 à 2003, responsable du pôle sécurité à Canal-Plus Technologies.
- Depuis 2003, maître de conférences à l'Université Paris 8, en charge des cours de cryptologie, d'histoire de la cryptologie et d'algorithmes algébriques dans le master Mathématiques et Applications.

Title of the preésentation : **Flatness and Submertivity in Discrete Time Dynamical Systems**

Summary of the presentation: The purpose of the presentation is to expose the links that exist between the notions of platitude, submersivity, reconstructibility, observability, controllability and reachability of dynamic discrete time systems. These notions will be presented and it will be particularly demonstrated that a submersive and flat discrete time dynamic system is necessarily totally controllable, this property being satisfied even when the system is nonlinear. The converse is true for linear systems but false in general.

This work was done jointly with Gilles Millérioux as part of the study on self-synchronizing encryption algorithms.

Résumé de la présentation : L'objet de la présentation est d'exposer les liens qui existent entre les notions de platitude, submersivité, reconstructibilité, observabilité, contrôlabilité et atteignabilité des systèmes dynamiques à temps discret. Ces notions seront présentées et il sera en particulier démontré qu'un système dynamique à temps discret submersif et plat est nécessairement totalement contrôlable, cette propriété étant satisfaite y compris lorsque le système est non linéaire. La réciproque est vraie pour les systèmes linéaires mais fausse en général.

Ces travaux ont été réalisés en commun avec Gilles Millérioux dans le cadre d'étude sur les algorithmes de chiffrement auto-synchronisants.

Bilal EL ALAMY

bilal.elalamy@equisafe.io

Présentation FR:
Diplômé de l'UPMC, Panthéon Sorbonne et ESCP Europe respectivement en physique, mathématiques appliquées à l'économie et la finance et management, Bilal a eu successivement des postes de chercheur en physique statistique dans les laboratoires de l'ESPCI-ParisTech, DataScientist à L'IRENA puis consultant en stratégie chez Accenture. Il se construit maintenant une expertise en crypto-finance qui l'a amené à fonder « EquiSafe », une entreprise technologique qui développe une banque d'investissement en ligne. Il aide aussi différents cabinets d'avocats à définir juridiquement des termes techniques en rapport avec la Blockchain et intervient en tant que Consultant externe sur la mise en place d'une stratégie blockchain pour des grands groupes financiers.

EN:
Graduated from UPMC, Pantheon Sorbonne and ESCP Europe respectively in physics, applied mathematics in economics and finance and management, Bilal successively held positions of researcher in statistical physics in the laboratories of ESPCI-ParisTech, DataScientist at IRENA (International Renewable Energy Agency) then strategy consultant at Accenture. He is now building a crypto-finance expertise that led him to found "EquiSafe", a technology-enabled investment bank. He also helps various law firms legally define technical terms related to Blockchain and acts as an external consultant on the implementation of a blockchain strategy for large financial groups.

- Title: **Blockchain for Social and Economic Empowerment**

Abstract: To apply blockchain technology to financials services various components needs to interact together and with off-chain services. Therefore, Identity Management, Automated compliance, capitalisation table management, and so on, needs to have implement privacy and network security by design in order to reach the value proposition that both tech, legal and finance brings together to renew the existing financial infrastructure and solve previous pain-points. Thus creating more trust, transparence and fairness in our daily activities as investors and issuers of securities. As finance power the economies, blockchain gives the opportunity to redefine the economics we want to put in place to fit social and national needs and inclusion.

All Papers

Introduction to STARKs: Scalable, transparent, and post-quantum secure computational integrity

Oualid Benamara
USTHB, Institute of Mathematics
benamara.oualid@gmail.com

***Abstract*—We review in this note a new class of zero knowledge proofs known as "Scalable, transparent, and post-quantum secure computational integrity" (STARK). We recall basic information theory concepts and outline important components of the STARK system.**

***Index Terms*—zero knowledge proofs, Reed Solomon codes**

I. INTRODUCTION

Zero knowledge systems are cryptographic schemes by which parties may prove computation integrity, ownership in given language or other computation problem without revealing sensitive information. Application of such scheme are possible for example in a server client set-up, wherein the server contains a database and a client wishes to check membership in the database. The server do not want to revel any sensible information regarding the database and the client want to ensure the correctness of the verification. Here the server can be represented as the prover and the client is the verifier.

Another example of ZK systems are computation integrity. Suppose that heavy computation need to be done on a smart phone. Due to space and power limitation of that device, such task cannot be possible. A solution to that is computation outsourcing procedure. If the computation are modelled by a function $F(x)$ wherein x is the smart phone input, then the smart phone sends x to a powerful server, the server computes $z = F(x)$ and send back z to the smart phone. Here ZK systems may provide a mean by which the smart phone can trust the sever regarding the computation integrity. Helpfully, the verification process is more efficient than computing the function F.

A lot of research been made for efficient ZK systems. Recently, efficient ZK system are reported such as SNARKs and STARKs. STARKs enhance the security model of SNARKs in the sense that that the former is secure even against computationally unbounded adversaries.

We introduce in the later section some notation from information theory. We then write formal definition of ZK systems. After that, we present the component on which STARKs are built, describing briefly how the reducing process is done.

II. NOTATIONS

1) **Turing Machines:** Informally speaking, a Turing Machine (TM) is a mathematical abstraction of the interaction and manipulation of a machine with data according to predefined rules.
2) **NP Proof System:** are defined as two TMs denoted the prover and the verifier. The prover will try to convince the verifier that $x \in NP$ by computing a proof y. The verifier check that $x \in NP$ using y without the knowledge of x, and output *accept* or *reject*. (NP are the class of problems that are difficult to solve but easy to verify)
3) **probabilistically checkable proofs (PCP):** Given a language L, then $L \in PCP$ if there exist an oracle machine (a special case of TM with access to an oracle), denoted $M^y(r, x)$, which solve an instance in the form $x \in L$.
4) **PCP of proximity:** Here instead of of checking for $x \in L$, we will check for that x is sufficiently close to the elements of L, with the notion of "close" defined by the mean of the notion of a "distance".
5) **Interactive oracle proof IOP systems:** consist of a couple of algorithms **(A,B)** which aims to prove membership in a relation $\mathcal{R}$ according to predefined probabilities.

III. ZERO KNOWLEDGE (ZK) SYSTEMS

ZK system S consists of two algorithms (P,V). P generates *proofs* of correct execution of a program C and V uses the *proofs* to check the correctness of the calculation. We note the following requirements:

- The running time of V is less than that of P, otherwise naive execution of the program C on the V side may be sufficient in case P has no confidential input.
- In case wherein C evaluate a function F with input w, w is called the *witness*.
- If executing of S reveals no information regarding the input w, then S is said *zero knowledge (ZK)*.

IV. ERROR CORRECTING CODES (ECC)

A. Principles

An ECC is a vector subspace V and denoted $[n, k, d]$:

1) **The length** is the length of the vectors v in V: $v = (v_1, \ldots, v_n)$.
2) **The dimension k** is the dimention of V.
3) **The minimum distance d:** Suppose that we have a mean of measuring the "distance" between two codewords v_1 and v_2, then

$$d = min_{(v_1, v_2 \in V)} d(v_1, v_2)$$

B. Reed Solomon Codes

Let $\mathbb{F}$ be a finite field and let S be a subset of $\mathbb{F}$. Let ρ be a parameter in the interval $(0, 1)$. We denote by $RS[\mathbb{F}, S, \rho]$ the *Reed Solomon* code. The codewords are functions $f : S \to \mathbb{F}$ that are evaluation of polynomials of degree less than $\rho|S|$, wherein $|S|$ is the number of element in the set S (the cardinal).

C. Coding and Decoding

V. Review of the literature

A. Probabilistically checkable proofs (PCP)

A language L ([1])is in $PCP(f(n), g(n))$ if if there is a polynomial time randomized oracle machine $M^y(r, x)$ such that:

1) It takes input x and a random string r of length $O(f(n))$, where $n = |x|$.
2) Generates a query set $Q(r, x) = \{q_1, \ldots, q_m\}$ of size $m = O(g(n))$.
3) Reads the bits $y_{q_1}, \ldots, y_{q_m}$.
4) Makes a polynomial-time computation on r, x and $y_{q_1}, \ldots, y_{q_m}$ and outputs $M^y(r, x) \in \{0, 1\}$ ($M^y(r, x)$ viewed as the output of the computation)

The PCP checks for $x \in L$. If we relax the above condition to *"x is sufficiently close to L"*, relative to a predefined distance, we obtain the so called *PCP of proximity*. Check [2] for formal definitions.

B. Interactive Oracle Proof (IOP) System

An IOP consists of two algorithms *(P,V)* which behave interactively, in k rounds, and output either 0 or 1 (accept or reject) [3].

VI. Languages and Binary Relations

A. Intuitive Introduction

Suppose we are in a client-server set-up. The client wishes to compute a function $F(x, w)$, on a public client input x and private server input w and output $z = F(x, w)$. The server then will use *zero knowledge proof* systems in order to convince the client that the output z is indeed the result of the calculation $F(x, w)$ (integrity concerns) without revealing any information about the confidential data w (confidentiality concerns).

B. Arithmetic Circuits Based Binary Relations

Definition: [4]Let n, h, l respectively denote input, witness and output size. The *circuit satisfaction problem* of a circuit $C : \mathbb{F}^n \times \mathbb{F}^h \to \mathbb{F}^l$ with bilinear gates is defined by the relation $R_C = \{(x, a) \in \mathbb{F}^n \times \mathbb{F}^h : C(x, a) = 0^l\}$ and its *language* is $L_C = \{x \in \mathbb{F}^n : \exists a \in \mathbb{F}^h, C(x, a) = 0^l\}$

C. Binary Relations for the STARKs Systems

1) The Class NTIME: The complexity class NTIME(f(n)) is the set of decision problems that can be solved by a non-deterministic TM which runs in time $O(f(n))$. Note that $NP = \cup_{k=0}^{\infty} NTIME(n^k)$.

2) The Computational Integrity (CI) Language: **Definition:** The binary relation R is the set of pairs (x, w) where

- $x = (M, x, y, T, S)$ with M a non deterministic TM, x and y are input and output and $T \geq S$ are time and space bounds.
- w are the set of steps of M such that $y = M(x)$ (y is the output for input x), under the constraints S and T.

Now we define the language L like this: $L = \{x = (M, x, y, T, S) | \exists w, (x, w) \in R\}$.

VII. The Reduction Process

Given statement in the form "α *is the result of executing* C *for* T *steps on input* x", the first step of the process is to reduce the above expression in the form of an *algebraic intermediate representation (AIR)*. The next step is to express the AIR representation in the *algebraic placement and routing (APR)* format, in which states of the AIR are represented as nodes on an affine graph. The last step is to transform the instance/witness of the APR to a pair of *Reed-Solomon proximity testing (RPT)* problem. This later is solved then using the *fast RS IOP of proximity (FRI)* protocol.

A. The Algebraic Intermediate Representation

An AIR instance is a tuple *x=(*$\mathbb{F}$*,T,w,P,C,B)*, wherein $\mathbb{F}$ is a finite field, T is the time constraint, w is an integer, P is a set of polynomials, C is a monotone circuit and B are a set of tuples representing boundary constraint in the form (i, j, α).

The witness are a set of polynomials $w_1, \ldots, w_n : 1, \ldots, T \to \mathbb{F}$ satisfying the constraints defined by the instance x.

Denote by BAIR the restriction of AIR to binary fields. It has been proved that BAIR admits a ZK-IOP [5]

B. The Algebraic Placement and Routing Problem

An instance in this setting is a tuple x=($\mathbb{F}$,T,N,Φ,L,L_{cmp},$\bar{\rho}$,ρ_{cmp}) wherein:

- $\mathbb{F}$ is a finite field.
- T is a set of indices.
- N is a subset of $T \times Aff_1(\mathbb{F})$.
- Φ is a subset of the set of functions $\mathbb{F} \times \mathbb{F}^N \to \mathbb{F}$. Notice that the expression $\mathbb{F}^N$ is the set of functions from N to $\mathbb{F}$
- L and L_{cmp} are affine subspaces of $\mathbb{F}$, $\bar{\rho}$ and ρ_{cmp} are sequence of rates.

A witness is a sequence of functions$w_\tau, \tau \in T$ satisfying the constraints defined by the instance, which are the following:

1) $\forall \tau \in T : w_\tau \in RS[\mathbb{F}, L, \rho_\tau]$.
2) $\forall \phi \in \Phi : \phi_N[w] \in RS[\mathbb{F}, L_{cmp}, \rho_{cmp}]$

The paper [5] states that there are algorithms that achieves the reduction from AIR into an APR instance/witness.

C. Binary RS Proximity Testing

Instances in this setting are the parameters of a Reed Solomon code $RS[\mathbb{F}, S, \rho]$. Witnesses are functions $w_{RS} : S \rightarrow \mathbb{F}$ and the satisfiability is defined by the relation $w_{RS} \in RS[\mathbb{F}, S, \rho]$.

The *algebraic linking IOP* (ALI) is used to reduce instances/witness of an APR into instances/witness in the BRPT.

The last phase is to run the *Fast RS IOP of proximity* IOPP to prove/verify instance/witness in the BRPT.

VIII. Conclusion

This paper presents a broad image of the STARKs systems, referring to other papers for detailed description. Unlike SNARKs for which an implementation is available freely on github, STARKs are not available as a concrete realization in code at the time of this writing. So this is an interesting subject to investigate.

References

[1] S. Arora, C. Lund, R. Motwani, M. Sudan, M. Szegedy. Proof Verification and Hardness of Approximation Problems

[2] E. Ben-Sasson, O. Goldreich, P. Harsha, M. Sudan, S. Vadhan. Robust PCPs of Proximity, Shorter PCPs and Applications to Coding

[3] E Ben-Sasson, A. Chiesa, and N. Spooner. interactive Oracle Proofs

[4] E. Ben-Sasson, A. Chiesa, E. Tromer, M. Virza. Succinct Non-Interactive Zero Knowledge for a von Neumann Architecture

[5] E. Ben-Sasson, I. Bentov, Y. Horesh, M. Riabzev. Scalable, transparent, and post-quantum secure computational integrity

Dual iris authentication system using Dempster-Shafer theory

Dr. Ghalem kamel ghanem
Ecole Préparatoire en Sciences et Techniques, BP 64 CH2 ACHABA HANIFI USTO 31000.
Oran, Algerie
ghalem.kamel@live.fr

Pr. Fatiha Hendel
Université des Sciences et de la Technologie d'Oran Mohamed Boudiaf, USTO-MB,BP 1505, El M'Nouer 31000
Oran, Algerie
fa_hendel@yahoo.fr

***Abstract*— In this paper, a dual iris authentication using Dempster Shafer theory is presented. The proposed method consists of three main steps: In the first one, the iris images are segmented in order to extract only half iris disc that contains relevant information and is less affected by noise. For that, we make a comparison between two detection techniques : Hough transform and Integrodifferential operator. We conclude that Hough transform is performant than the Integrodifferential operator. The segmented images are normalized by Daugman rubber sheet model. In the second step, the normalized images are analyzed by two techniques: a bench of two 1D Log-Gabor filters and Haar wavelet to extract the texture characteristics. The results affirm that 1D Log-Gabor filter is efficient than Haar wavelet. The encoding is realized with a phase of quantization developed by J. Daugman to generate the binary iris template. For the authentication and the similarity measurement between both binary irises templates, the hamming distances are used with a previously calculated threshold. The score fusion is applied using Dempster Shafer rule. The proposed method has been tested on a subset of iris database CASIA-IrisV3-Interval. A dual iris authentication system outperforms the others methods.**

Keywords*— *Biometric, iris, fusion, Dempster-shafer theory, authentication

NOMENCLATURE

CCD Charge-coupled device
DS Dempster-Shafer
EER Equal Error Rate
FFT Fast Fourier Transform
FAR False Accept Rate
FRR False Reject Rate
IFFT Inverse Fast Fourier Transform
ROC Receiver Operating Characteristic

$\boldsymbol{X_j}$ Tow iris codes
$\boldsymbol{Y_j}$
$\boldsymbol{N}$ is the number of bits in each iris code
$\boldsymbol{f_0}$Central frequency of 1D log Gabor filter
G(f) Frequency response of 1D log Gabor filter
σ The standard deviation of the 1D Log-Gabor wavelet
⊕ XOR operator
∩ AND operator
HD Hamming distance between two iris templates

I. INTRODUCTION

The biometric includes different biometric modalities; Contrary to the way that we have and that we can, therefore, lose (a key) or what we know and that we can in this way forget (a password), the biometric modalities speak to what we are and permits to prove our identity.
Fingerprint, hand geometry, iris, retina, face, palmprint, ear, DNA, voice, signature, keystroke are different biometric modalities.

However, the unimodal biometric systems using one biometric modality for recognition cannot guarantee at present an excellent recognition rate. Furthermore, Furthermore, these systems suffer from limitations such as sensitivity to noise, data quality, non-universality and spoof attacks. To overcome these problems, Multimodal biometric systems which combine multiple biometric signatures have been developed on purpose to achieve a better recognition rate.

Fusion of the biometric traits can be done at different stages of recognition system as following:

A. Fusion at feature extraction level

The data is acquired from each sensor is utilized to generate a feature vector. Then, the features are fused to form one feature vector.

B. Fusion at matching score level

The matching score of each system is combined and compared with the stored template.

C. Fusion at decision level

The final decision is taken from a result of each system. Thus, the individual is accepted or rejected.

In this work, the researchers tried to evaluate the performance of dual iris authentication system in terms of accuracy and mitigate the errors using a most standard fusion technique: score level fusion. Furthermore, a dual iris identification system is elaborated using support vector machine.

The remainder of this paper is organized as follows. Related work is presented in section II. A proposed method is

detailed in section IV. Experimental results are given in section V. Finally, conclusions are drawn in section VI.

II. RELATED WORK

The texture of iris is a combination of several elements that make it one of the richest distinctive textures of the human body. It has ligament arches, crypts, ridges, furrows, and ruffles. The location of these components, the crossing between them and the shape that can have these elements make that the texture of iris is considered as one of the richest of biometrics.

Daugman's algorithm [1] is the best iris algorithm known in biometrics. The algorithm consists of segment iris using Integro-Differential Operator and iris normalization is implemented using Daugman's polar representation. Then, iris encoding is applied using 2D Gabor filters to extract a binary code of 256 bytes. The Matching is processed by computing similarity between two iris codes using Hamming Distance. The more Hamming Distance is small, the more both codes are similar. A distance of 0 corresponds to a perfect match between both iris images, while two iris images of different person will have a Hamming Distance close to 0.50.

In 1997, Wildes [2] proposed an alternative and completely different method compared to Daugman's algorithm [1]. The iris is acquired from a CCD Camera in low luminosity. Then, iris is segmented using Circular and Elliptic Hough transform and is normalized using a transformation function of pixels. After that, Iris is filtered using Laplacian of Gaussian filters with four different resolution levels. A normalized correlation is calculated for every resolution levels. The median of the values of correlations is computed for the filtered image. The fusion of four values is applied using Fisher's linear discriminant.

In 1998, W. Boles and B. Boashash [3] proposed a new approach for recognition of individuals from iris images. The algorithm is insensitive to variation in the lighting conditions and noise levels. A Median filter is used for preprocessing. The advantage of this technique is to extract a features vector from 1D signals rather than 2D images analyzed in [1], [2] using zero-crossings of the dyadic wavelet transform at various resolution levels. Only a few selected intermediate resolutions are used for matching. The matching is applied using different dissimilarity functions. Thus make algorithm faster and less sensitive to noise and quantification error. Since, then many others iris recognition methods have been published in literature but the realization of a system which performance is similar to Daugman's system was hard to achieve. On the other hand, a method which performance is close to Daugman's approach is detailed in [4].

In 2004, Ma et al. [4] presented an efficient algorithm for iris recognition. The iris region is located by Canny Filter and Hough Transform. Then, the iris is enhanced by histogram equalization and is normalized. A 1D Wavelet Transform is used to represent resulting 1D intensity signals. The position of local sharp variation points is registered as features. The similarity function (exclusive or operation) is used for Matching. This algorithm is efficient and faster than Daugman'salgorithm [1].

The above iris recognition methods may be considered "conventional" since they require very important cooperation from the subject, particularly in the enrollment phase, where the time required for registration of a user's can be considered important.

In [5], the authors presented a novel iris verification system. An image enhancement is applied using curvelet transform after the eye detection. The contourlet transformation is carried out for feature extraction. The classification is performed using adaptive neuro-fuzzy inference system showed a good performance in terms of accuracy and processing time.

In [6], the authors proposed a modified Masek approach as well as a comparative study of the performance of the following methods: radial segmentation, Masek segmentation approach, modified Masek approach. The proposed method tested on the CASIA Iris Database V3.0 showed a good performance in terms of accuracy and processing time.

The authors in [7] proposed an efficient iris detection method for iris images captured in unconstrained environment. A iris image includes noises such as specular reflections, eyeglasses, low contrast, low illumination and occlusions by eyebrow hair, eyelids and eyelashes. Thus, a morphological operation is applied to eliminate specular reflections. The pupil is detected byDaugman's integrodifferential operator (IDO). On the other hand, the iris is detected by proposed modified Daugman's IDO. The proposed method is based on a thresholding and morphological operation to optimize the detection process of pupil. The proposed method is tested with CASIA-Iris-Thousand V4 iris database which contains noisy iris images. Accuracy of the proposed method is 99.3% and processing time is 1.86 seconds per image.

In [8], the authors proposed an efficient iris segmentation technique Fuzzy C-means clustering tested on UBIRIS V2 which contains noisy iris images including specular reflections, pupil, eyelids and eyelashes.

In this paper, we try not only to combine the advantages of the described methods, but also to improve overall performance. In this perspective, researchers have used more than one biometric trait, and thus, the multibiometric systems have emerged. Numerous multi-biometric systems have been developed which fusion is made Matching score.

In [9], the authors presented a multimodal system of identification combining the iris and the fingerprint. A stage of modeling based on Artificial Immune Recognition System is tested, a good performance were achieved.

In [10], the authors presented a framework for multimodal biometric fusion based on the uncertainty concept of Dempster-Shafer theory. A combination of quality measures and the accuracy of classifiers (equal error

rate) are proposed to encode the uncertainty concept to improve the fusion. The proposed method revealed a good performance with an EER equal to 1 %.

In [11], the authors presented a novel fusion method at matching score called Choquet integral tested on face and fingerprint. The proposed method tested on fingerprint showed a recognition rate of 99.94% which is much better than the sum rule method with the best normalization method (i.e. min-max normalization) that gives 99.88%.

In [12], the authors presented a hybrid fusion scheme based on feature, score and decision level. The final decision is done by fusion of three classifiers with a decision rule called Majority voting. The face and iris feature extraction is applied using global and local feature extraction methods. Then, a feature level fusion individually for face and iris is applied to generate face and iris classifiers. A score level fusion is applied between LDA method for face and LBPH method for Iris. The decision level fusion is applied for three classifiers with a decision rule called Majority voting. The experimental results showed a good recognition rate equal to 98.75%.

Above multi-biometric systems show very good performance. While dealing with two or more different algorithms increase the systems complexity. To solve this problem, the authors propose to deal with just one algorithm using both irises of the same person. The most important recent works to our knowledge that deal with the biometric recognition of person from the both eyes are:

In [13], the authors proposed a novel approach for iris recognition using both eyes. The iris is detected using Hough transform and is normalized using pseudo-polar transformation. The feature extraction is performed using Discrete Wavelet Transform at two-level. The approximate image is divided into 8x8 blocks at first level and 4×4 blocks at second level then the mean is calculated and combined in each block to generate the feature vector. The classification is carried out using neural networks (MLP) on the feature vectors containing 184 and 96 coefficients. Learning is applied to the feature vectors extracted from the left and right iris while for the test can be applied either on the left or right iris. The experimental results showed a recognition rate equal to 100% tested on 3 individuals from the CASIA Iris database V3.

In [14], the authors proposed a new approach for recognition using both irises. The iris is segmented using Canny filter and Hough transform, then the segmented iris is normalized by J. Daugman's rubber sheet model. The iris feature extraction is carried out using convolution of the normalized iris with 1D Log-Gabor filters then the phase of filtered iris is quantized in order to generate a binary code. A Hamming distance is used for Matching. Matching operation consists of comparing the two iris feature vectors of a person with the others; if the Hamming Distances are less than the threshold then the person is identified. A experimental results showed a good recognition rate equal to 99.92% with an FNR = 9.96%, while for unimodal systems (left iris and right iris) the recognition rate is equal to 99.87% with an FNR = 14.62% and FNR = 15.68%.

This paper proposes a dual iris authentication and identification systems that follow these main phases:

1. Segmentation based on circular Hough transform to delineate iris and pupil circles.

2. Normalization stage was applied to compensate the non-concentricity of the two borders and the varying size of the iris caused by the dilation/contraction of the pupil.

3. A bench of two 1D Log-Gabor filters is used for extracting information from iris texture, and then the encoding is realized with a quantization phase developed by Daugman [1].

This work presents a contribution related to the iris segmentation phase. This contribution consists of extract only the interior half of the iris disc rather than the whole iris disc which contains the most relevant information and it is less affected by noise. In addition, a dual iris authentication system is developed using Dempster Shafer theory and a dual iris identification system is established using as a classifier: support vector machine. The systems are tested on CASIA-IrisV3-Interval.

III. PROPOSED METHOD

The proposed method is composed of four main stages: preprocessing, feature extraction, fusion, and matching.

A. Preprocessing Stage

First, the eye images require going through the preprocessing phase including segmentation and normalization.

1) Iris Segmentation

The segmentation of iris is realized by two commonly Edge detector method: Hough transform (Fig.1), Operator integro-differential(Fig.2)

a) Hough transform

1. Iris image is smoothed using a Gaussian filter with size 13 x13 pixels, and standard deviation $\sigma = 2$.
2. We calculate Horizontal gradient and vertical Gradient using:

$$G_V = \begin{matrix} -0.5 & 0 & 0.5 \\ -1 & 0 & 1 \\ -0.5 & 0 & 0.5 \end{matrix}, G_H = \begin{matrix} -0.5 & -1 & -0.5 \\ 0 & 0 & 0 \\ 0.5 & 1 & 0.5 \end{matrix}$$

The vertical Gradient is used to detect iris-sclera boundary. The vertical and horizontal gradient is used to detect iris-pupil boundary.

The gradient is calculated using the following equation:

$$|G| = \sqrt{G_x^2 + G_y^2} \quad (1)$$

3. The local maxima are suppressed and finally, we obtain a binary image using Hysteresis threshold.

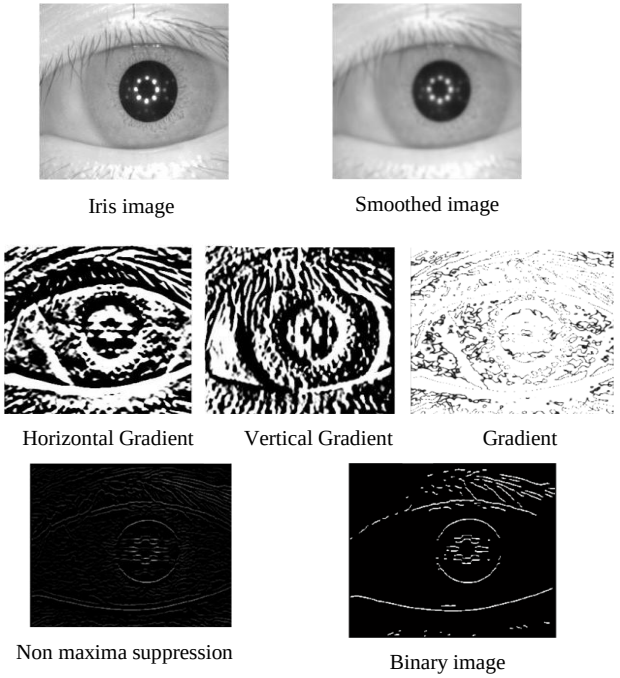


Fig. 1. Detection of iris disc using Hough transform

b) Integrodifferential operator

ALGORITHM

Begin
Read iris image
Eliminate specular reflection
Detect iris center and rayon
  Begin
  Detect circles
  Calculate gradient
    If Gradient>maximum
      Select circle
    Else
    Change center and rayon
  End
Repeat for pupil
End

In this work, the objective is to extract only relevant information from iris, which is represented by the structural variation of the iris texture (high gradient areas), only the internal half of the iris disc is exploited rather than whole, because it contains the most relevant information [19] and it is less affected by the noise. Indeed, the proposed technique decreases the complexity and the computation load without losing information (as shown in Table I).

TABLE I. COMPARAISON : TOTAL IRIS DISC VS HALF IRIS DISC.

	ACCURACY (%)	PROCESSING TIME FOR ONE IRIS IMAGE (%)
TOTAL IRIS DISC	99.87	22.88
HALF IRIS DISC	99.96	12.37

Discussion

From Table. I, we denote that treatment using only half iris disc is more efficient with an accuracy of 99.96% and processing time for one iris image of 12.37 s than the treatment using a whole iris disc with accuracy 99.87% of and processing time of 22.88 s.

TABLE II. COMPARISON : HOUGH TRANSFORM VS OPERATOR INTEGRODIFFERENTIAL [20]

	Hough transform	**Operator integrodifferential**
Accuracy (%)	99.95	99.42
FAR (%)	0	0
FRR(%)	6.10	85.25
EER(%)	0.92	13.5
Processing time (s)	1.31	1.56

Discussion

From Table II, we denote that Hough Transform is more efficient than Operator integro-differential in terms of Accuracy, Error (FAR, FRR, EER), Processing time. The Hough transform gives an accuracy rate of 99.95%, FAR of 0%, FRR of 6.10%, EER of 0.92%, the Processing time for one iris image of 1.31s. While, Operator integro-differential gives an accuracy rate of 99.42%, FAR of 0%, FRR of 85.25%, EER of 13.5% and processing time of 1.56%.

We conclude that The Hough transform is more reliable and fast than Integro-differential Operator. Therefore, the Hough Transform is used for segmentation of iris.

2) Iris Normalisation

The iris disc does not always have the same dimension, even for eye images of the same person; this is due to various problems as follows:

1. Different acquisition conditions of the eye images. Dilation and contraction of the pupil due to the variation of the illumination level.
2. The circles of iris and pupil are not concentric.

In order to overcome these problems, a stage of normalization is applied. It consists of transforming the region of the iris disc to rectify the dimensions of all the iris discs, by using the homogenous rubber sheet model proposed by Daugman [10]. It transforms each point in the iris area to the polar coordinates (r,θ), where *r* is on the interval [0,1] and θ is angle [0,2π], as illustrated in Fig.2.

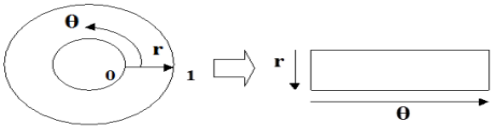


Fig. 2. Daugman rubber sheet model [10].

In our system, (20*240) points were used, but only (10*240) points corresponding to the internal half of the iris disc that contains the most relevant information and which is less affected by noise [15], are retained for the next steps of the processing, as shown in Fig.3.

Fig. 3. Normalization of the segmented iris.

B. *Feature Extraction Stage*

After that, the feature extraction stage is applied in purpose to extract the most discrimination information present in the iris region. For this reason, two filters are used Log-Gabor 1 D and Haar wavelet.

1) Log-Gabor 1D filter

The Fast Fourier Transform is applied for each line of the normalized matrix image (FFT to 1D signals).

Then, the Inverse Fast Fourier Transform IFFT is applied on the multiplication FFT (1D signals) by a 1D Log-Gabor Filter.

The frequency response of a 1D Log-Gabor filter is given by:

$$G(f) = \exp\left(-\frac{\log(\frac{f}{f_0})^2}{\log(\frac{f}{f_0})^2}\right) \quad (2)$$

a) Parameters setting

- A bench of two 1D Log-Gabor filters is used.
- The standard deviation of the 1D Log-Gabor wavelet is given by $\sigma = 2$.
- The center frequency of the 1D Log-Gabor wavelet is given by $f_0 = 0.05$.

Indeed, the phase of a filtered image was quantized using four-quadrants of Daugman [1], when going from one quadrant to an adjacent quadrant, one bit is changed as shown in Fig. 4.

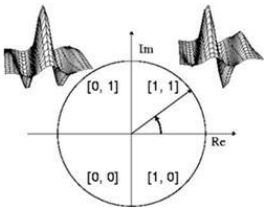


Fig. 4. Quantization Phase [1].

The encoding process produces a bitwise template containing a number of information bits (as shown in Fig. 5), the total number of bits in the template (9600 bits) will be the angular resolution (240) times the radial resolution (10), times 2, times the number of filters used (2).

Fig. 5. Iris code.

2) Haar wavelet

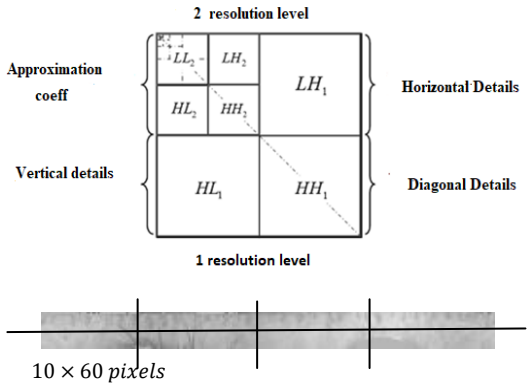
a) Algorithm

```
For each individual indv
  For each iris trc of individual indv
    Decompose iris {indv, trc} into 4 region
     For each region of iris {indv,trc}
          Extract approximation coeff into 4 resolution level
          Extract vertical details into 4 resolution level
     Fin
     Concatenate approximation coeff, vertical details (I)
% Binarization of I
      [x,y]=size(I)
      For i=1:x
      For j=1:y
            If I(i,j)>0
               I(i,j)=1;
            Elseif
              I(i,j)=-1 ;
            Endif
            End
        End
     save I
  End
End
```

The obtained iris code is shown in Fig.6.

Fig. 6. iris code

The normalized iris is decomposed into 4 regions. For each region, approximation coeff and vertical details are extracted into four resolution level 4x(1x4 pixels). After concatenation and binarization. The iris code has a dimension of 32bits (as shown in Fig.7).



1 Level resolution 5×30 pixels
2 Level resolution 3×15 pixels
3 level resolution 2×8 pixels
4 Level resolution 1×4 pixels

Fig. 7. Decomposition of Iris normalised.

TABLE III. COMPARISON: LOG-GABOR 1D VS HAAR WAVELET

	Log-Gabor 1D filter	**Haar wavelet**
Accuracy (%)	99.95	99.32
FAR (%)	0	0
FRR(%)	6.10	100
EER(%)	0.92	20
Processing time (ms)	14	17

Discussion

From Table III, we denote that Log-Gabor 1D filter is more reliable than Haar wavelet in terms of Accuracy, Error (FAR, FRR, EER), Processing time. The Log-Gabor 1D filter gives an accuracy rate of 99.95 %, FAR of 0%, FRR of 6.10%, EER of 0.92%, the Processing time for one iris image of 14ms.In the otherwise, The Haar Wavelet gives an accuracy rate of 99.32%, FAR of 0%, FRR of 100%, EER of 20% and Processing time of 17ms.

We conclude that The Log-Gabor 1D filter is more efficient and fast than Haar wavelet. Therefore, the Log-Gabor 1D filter is used for Feature extraction of iris.

C. Matching Stage

The matching consists to compare two iris code using Hamming distance. The Hamming Distance (HD) is defined by:

$$HD = \sum_{j=1}^{N} X_j \oplus Y_j \quad (3)$$

Where X_j and Y_j are the two bitwise iris code, N is the number of bits in each iris code. Literally, the Hamming distance calculates the number of different and valid bits for the two iris code between X_j and Y_j.

The number of translation bits that compensates for the rotation of the iris needs to be fixed. We applied a translation of the iris code in an interval [-3, +3] bits. We take into consideration the minimum Hamming distance.

D. Fusion Stage

In this stage, score level fusion was applied on goal to improve the performance of the dual iris system.

1) Score Level Fusion

Matching score level fusion combines the scores generated by multiple classifiers relating to the left and right iris to affirm the veracity of the claimed identity.

The DS theory of evidence [16] is a powerful tool for representing uncertain knowledge.

DS theory can be considered as a generalization of probability theory and employs degrees of belief (or mass, a generalization of probability). DS theory can be used to combine evidence obtained from multiple sources of the system to compute the probability of an event.

The fusion scores using Dempster-Shafer (DS) theory is carried out to combine the scores obtained from both irises ($S^{Left\ iris}$, $S^{Right\ iris}$) in purpose to improve the overall performance.

Combination rule: The two evidence sources $m_1(S^{Left\ iris})$ and $m_2(S^{Right\ iris})$ can be combined to obtain the belief mass committed to C ϵ Θ according to the following combination or orthogonal sum [16] :

$$m_{12}(C) = m_1(C) \oplus m_2(C) \quad (4)$$

$$m(C) = \frac{\sum_{S^{Left\ iris} \cap S^{Right\ iris} = C} (m_1(S^{Left\ iris}) m_2(S^{Right\ iris}))}{1 - \sum_{S^{Left\ iris} \cap S^{Right\ iris} = \emptyset} (m_1(S^{Left\ iris}) m_2(S^{Right\ iris}))} \quad (5)$$

When $C \neq 0$. The denominator is a normalization factor, which intuitively measures how much $m_1(S^{Left\ iris})$ and $m_2(S^{Right\ iris})$ are conflicting.

IV. Experimental Result

A. Simulation Environment

The proposed method has been tested on a subset of iris database CASIA-IrisV3-Interval [17] in order to evaluate its performance in authentication mode. The subset contains 1180 eye images of 118 individuals (classes), and each individual has five iris samples for the left eye and five iris samples for the right eye.

B. Performance Metrics

- False Reject Rate (FRR): also known as Type I error, is the measure of the probability that the biometric security system will incorrectly reject an access attempt by an authorized user.

- False Accept Rate (FAR): also known as Type II error, is the measure of the probability that the biometric security system will incorrectly accept an access attempt by an unauthorized user.

- EER (Equal Error Rate): The EER is the operating point for which the False Reject Rate (FRR) is equal to the False Accept Rate (FAR).

C. Decidability

Decidability [1] is the best metric which indeed takes into account the mean and standard deviation of the intra-class and inter-class distributions:

$$d' = \frac{|\mu_s - \mu_d|}{\sqrt{\frac{(\sigma_s^2 + \sigma_d^2)}{2}}} \quad (6)$$

Decidability d' is a distance in standard deviations calculated using Eq. (6) which is a function of the magnitude of the difference between the mean of the intra-class distribution μ_s, and the mean of the inter-class distribution μ_d, the standard deviation of the intra-class and inter-class distributions, σ_s, and σ_d respectively.

TABLE IV. DECIDABILITY TABLE FOR VARIOUS NUMBERS OF BIT-SHIFTS

Number of shifts	μ_s	σ_s	μ_d	σ_d	d'
0	0.3300	0.0723	0.4914	0.0284	3.4314
1	0.3137	0.0697	0.4860	0.0279	3.8149
2	0.3072	0.0668	0.4812	0.0269	4.0264
3	0.3044	0.0653	0.4772	0.0258	4.0742
4	0.3032	0.0646	0.4738	0.0247	4.0431
5	0.3028	0.0642	0.4709	0.0238	3.9907
6	0.3025	0.0639	0.4684	0.0230	3.9362
7	0.0637	0.0642	0.0223	0.0216	3.8862
8	0.3023	0.0635	0.4645	0.0216	3.8303
9	0.3022	0.0634	0.4629	0.0211	3.7999
10	0.2758	0.0639	0.4643	0.0201	4.3960

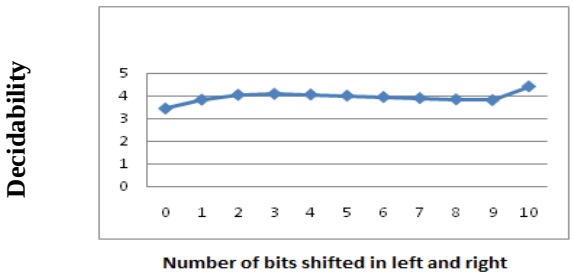


Fig. 8. Decidability curve for various numbers of bit-shifts

Using Eq. (6), several different decidability are found out using 0-bit shift to 10-bit shift towards both left and right iris templates.

The higher decidability is equal to 4.0742 at 3-bit shift (as shown in Table IV and Fig. 8) that guarantees good separation of intra-class and inter-class distributions, which allows for more accurate recognition.

D. Dual Iris System

1) Score Level Fusion

Matching score level fusion combines the scores calculated by Hamming distance relating to the left and right iris to affirm the veracity of the claimed identity. The Dempster Shafer theory of evidence [16] is a powerful tool for representing uncertain knowledge.

The fusion scores using Dempster-Shafer (DS) theory is carried out to combine the scores (Hamming distance) obtained from both irises (in purpose to improve the overall performance.

a) Algorithm

For each individual **indv**

For each different iris , j : such as i, j belong to iris set of individual **indv**

Calculate the score $S_g(i,j)$=1−DH_g(i,j)

Calculate the score $S_d(i,j)$=1−DH_d(i,j)

Calculate the fusion of score

$$S_f(i,j) = \frac{S_g(i,j) \times S_d(i,j)}{1 - \left(\left(1 - S_g(i,j)\right) \times S_d(i,j)\right) + \left(1 - S_d(i,j) \times S_g(i,j)\right)}$$

k=1
For s=0:0.05:1
If $S_f(i,j) < s$ then
FN(k) = FN(k) + 1 %False Negatif
$k = k + 1$
End if
End
End
End

For each different individual **indvi**,
For each different iris (i,j) such as i belong to iris set of individuals **indvi** and j belong to iris set of individuals **indvj**

Calculate the score $S_g(i,j)$=1−DH_g(i,j)

Calculate the score $S_d(i,j)$=1−DH_d(i,j)

Calculate the fusion of score

$$S_f(i,j) = \frac{S_g(i,j) \times S_d(i,j)}{1 - \left(\left(1 - S_g(i,j)\right) \times S_d(i,j)\right) + \left(1 - S_d(i,j) \times S_g(i,j)\right)}$$

k=1
For s=0:0.05:1
If $S_f(i,j) \geq s$ then
FP(k) = FP(k) + 1 %False positif
k=k+1
End if
End
End
End

maxindv= number of individuals nbtr=number of iris images per individual

nbinter=maxindv×(nbtr×(nbtr−1)⁄2)

nbintra=maxindv×(nbtr×(nbtr−1)/2) TN=nbinter−FP(True Negatif)

nbintra = maxindv × (nbtr × (nbtr − 1)/2)

TN = nbinter − FP %True Negatif

TP = nbintra − FN % True Positif

TPR = (TP / nbintra) × 100 %True Positif Rate

TNR = (TN / nbinter) × 100 % True Negatif Rate

FAR = (FP / nbinter) × 100 %False Accept Rate

FRR = (FN/nbintra) × 100 %False Reject Rate

Accuracy = ((TP + TN)/(nbintra + nbinter)) × 100

The dual iris system using score level fusion achieves an accuracy of 99.62% at decision threshold of 0.64 (as shown in Fig. 9) with FAR of 0.36%, FRR of 1.61%, EER of 1.36% (as shown in Fig. 10) and processing time of 12.36 s for one iris image.

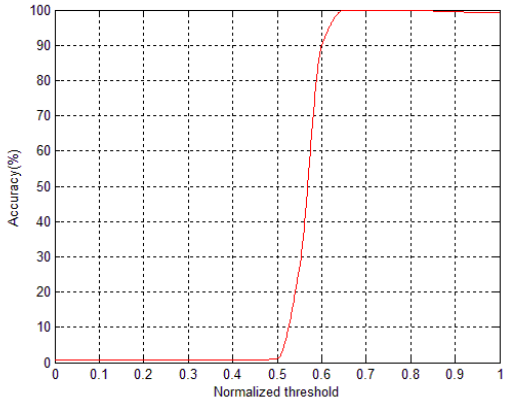


Fig. 9. The accuracy of the dual iris system.

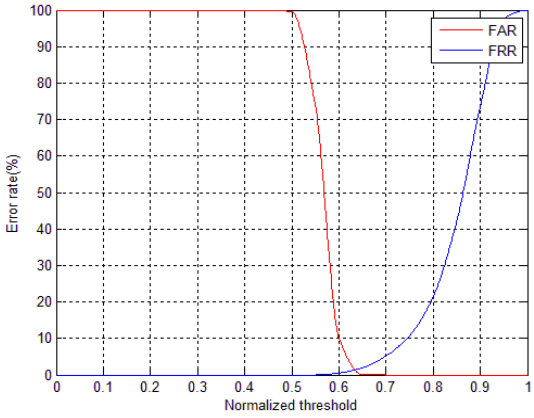


Fig. 10. FRR and FAR of the dual iris system

TABLE V. SYSTEM ACCURACY AND FRR FOR VARIOUS APPROACHES.

Iris authentication approaches	Accuracy (%)	FAR (%)	FRR (%)	EER (%)
Daugman approach [1]	99.90	0.01	0.09	-
LDA-based approach [18]	99.14	0.00	0.69	-
Iftakhar and Ashraful Approach[14]	99.92	0.00	9.96	-
Proposal dual iris authentication	99.96	0.00	6.10	0.92

Discussion

As it clear from Table V, the proposed dual iris authentication gives satisfactory results in term of overall performance (Accuracy, FAR, FRR, EER) compared to other approaches. The proposed method uses only half iris disc that contains the most relevant information and it is less affected by noise, contrary to other detection methods and represents the uncertainty in the form of the probability of the evidence, which allows the system a degree of confidence while Iftakhar and al [14] uses the fusion method based on the AND rule which is more drastic and leads to improve the FPR. In addition, LDA-based approach proposed by Chu and Chen [18], uses a probabilistic neural network (PNN) and require a training algorithm which increases the computational load.

V. CONCLUSION

The purpose of this work was to find out a dual iris authentication that guarantees a good performance and to make sure that there is no false acceptance rate, which promises useful security applications. The proposed method consists in segmenting, to normalizing, characterizing and encoding the iris. For the segmentation part, the detection of the iris/pupil circles was performed by Hough circular transform. Only the interior half of the iris disc containing the most relevant information and less affected by noise, which reduces time complexity was extracted. Iris normalization part was performed by the Daugman rubber sheet model with a resolution of 10×240. This stage was analyzed by the bench of two 1D Log-Gabor filters to extract the texture characteristics and the encoding was realized with a phase of quantization developed by J. Daugman to generate the binary iris template. For the authentication and the similarity measurement between both binary irises templates, the hamming distances are used with a previously calculated threshold. The score fusion is applied using Dempster Shafer rule. The experimental results show that the proposed system gives a good performance compared to others approaches with an accuracy of 99.96%, FAR of 0%, FRR of 6.10%, EER of 0.92% and processing time for one iris image of 12.37 s.

REFERENCES

[1] J. Daugman, How iris recognition works, *IEEE Trans.Circuits Syst. Video Techn*, 14, pp. 21-30, 2004

[2] R. P. Wildes et al., A machine-vision system for iris recognition, *Machine Vision and Applications*, 9, pp. 1-8, 1996

[3] W. W. Boles and B. Boashash, A human identification technique using images of the iris and wavelet transform, *IEEE* Transactions on Signal Processing, 46, pp. 1185-1188, 1998.

[4] L. Ma et al., Efficient iris recognition by characterizing key local variations, IEEE Transactions on Image Processing, 13, pp. 739-750, 2004.

[5] Sumathi, T., Karthikeyan, T., An Improved Identification System Using Iris Based on Curvelet Transform and WBCT, *International Review on Computers and Software (IRECOS)*, 9(8), pp. 1320-1327, 2014.

[6] Aydi, W., Masmoudi, N., Kamoun, L., A Fast and Accurate Circular Segmentation Method for Iris Recognition Systems, *International Review on Computers and Software (IRECOS)*, 9 (3), pp. 468-477, 2014.

[7] Kumar, V., Asati, A., Gupta, A., Iris localization based on Integro-Differential Operator for unconstrained infrared iris images, *International Conference on Signal Processing, Computing and Control*, pp. 277– 281, 2015.

[8] N. Kaur, M. Juneja, segmentation approach for iris recognition in less, constrained environment, *Lecture Notes in Electrical Engineering*, 335, pp. 481-490, 2015.

[9] Benchennane, I., Hadjar, A., Benyettou, A., Individuals Identification Using Artificial Immunes Systems, *International Review on Computers and Software (IRECOS)*, 10 (1), pp. 20-26, 2015.

[10] K. Nguyen, S. Denman, Score-Level Multibiometric Fusion Based on Dempster-Shafer Theory Incorporating Uncertainty Factors, *IEEE Transactions on Human-Machine Systems*, 45, pp.132-140, 2015.

[11] Fakhar, K., et al. Biometric Score Fusion in Identification Model using the Choquet Integral *International Conference on Electrical and Information Technologies* pp, 233–236, 2015.

[12] Azom, V., Adewumi, A., Tapamo, J.R., Face and Iris biometric person identification using hybrid at feature and score-level, *International Conference (PRASA-RobMech)* pp, 207–2012, 2015.

[13] Sharkas, M., A Neural Network Based Approach for Iris Recognition Based on Both Eyes, *SAI Computing Conference*, pp. 233–236, 2016.

[14] Iftakhar, H., Minnatul, F., and Ashraful Amin, M., Dual Iris Based Human Identification, *Proceedings of 14th International Conference on Computer and Information Technology*, 2011.

[15] Feddaoui, N., et Hamrouni, k., Reconnaissance de l'iris par filtrage de Gabor et deux variantes de descripteurs de texture, *TAIMA* , 2000.

[16] G.Shafer, *A Mathematical Theory of Evidence*, Princeton,NJ,USA Princeton Univ. Press,1976.

[17] Iris database CASIA-IrisV3, Chinese Academy of Sciences—Institute of Automation. Retrieved on Dec 2011. http://www.cbsr.ia.ac.cn/IrisDatabase.htm.

[18] C.T. Chu , C. Chen, "High performance iris recognition based on LDA and LPCC," In: Proceedings of the 17th IEEE International conference on tools with, artificial intelligence (ICTAI 05), pp 417–421,2005.

modeling and non linear dynamic analysis of the chaotic Colpitts oscillator up to 1 GHz

C. Rouifed[1,2]
[1] Mouloud mammeri university of tizi ouzou,
tizi ouzou,
Algeria.

A. Ouslimani[2,] M. Laghrouche[1]
[1]Mouloud mammeri university of tizi ouzou,
tizi ouzou, algeria.
[2] Ecole nationale supérieure de l'électronique et ses applications, Cergy, France

Abstract
—In this paper, we consider a Colpitts oscillatos as a model for nonlinear dynamic analysis. In particular, we perform a bifurcation analysis using a real and theorical model of the Colpitts oscillator. This analysis, simulated with Matlab, shows a difference between the two models while calculating their parameters. Moreover, in order to fixe the optimal values of the circuit's component, spectrum simulation under ADS have been performed up to 1GHz. It shows a chaos bandwidth of 600 MHz.

Keywords-component; Colpitts osccillator; bifurcation diagram; chaotic system

I. INTRODUCTION

The first demonstration of a chaotic system generated by a linear circuit has been achieved in 1983, it is the so-called "Chua's circuits" [1]. On the other hand, this chaotic signal could be also generated using non-linear systems, however oscillators are strongly depending on the initial conditions of the system but could be controlled to achieve the desired chaotic signal [1-2]. This important propriety paves the way to introduce such signals in the information coding system. Among the electronic circuits that fulfill this function, Colpitts oscillator is an interesting circuit with high non-linearity behavior and wide bandwidth [3-4-5]. These proprieties are the key enabling factors to implement such circuits in communication systems addressing coding and modulation [6].
It has been demonstrated in the bifurcation theory, the normal forms and the technique of communication could be useful to qualitatively characterize the different dynamic behavior shown by this oscillator [7]. The approach that has been followed to obtain different equilibrium behaviors consists in selecting a model of the circuit which minimizes the main characteristics of the real Colpitts oscillator. Furthermore, we emphasize that the complex bifurcation structure exposed by the Colpitts oscillator gives a link to coexistence phenomena in a large area of parameter space. This paper is organized as flow: section 2: the real model of Colpitts oscillator and the bifurcation diagram are studied. Section 3: we present the ideal model and we give the model based in ADS. As a conclusion, a comparison between the two models is reported in section 4.

I. NONIDEAL MODEL

We consider the circuit configuration depicted in Figure. 1. The circuit is biased by Vcc and the current I_0 with a conductance G_0 [7].

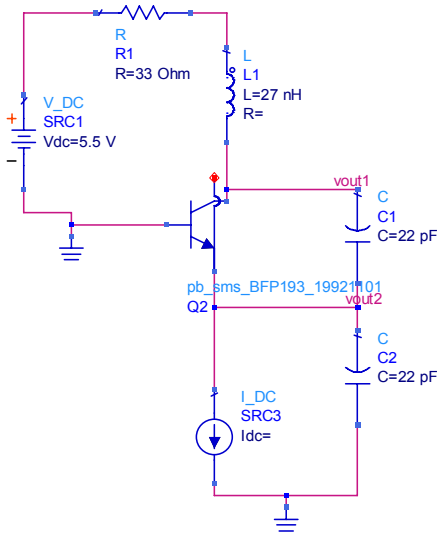


Fig.1 : circuit diagram of chaotic colpitts oscilator

We consider the passive elements and the active element are neglected and the nonlinear model of the emitter base is presented by the following equation [9]:

$$f(-V_{C2}) = I_s exp\left(\frac{-V_{C2}}{V_T}\right) \quad (1)$$

With α is common base forward short-circuit current gain of the transistor.
After some transformations in the equations of states for the schematic in figure.1. [8], they can be written as follows:

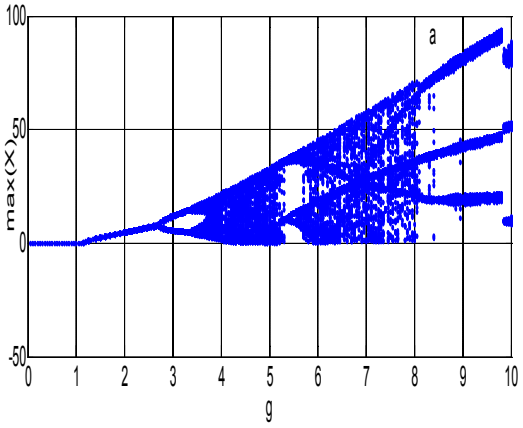
$$\begin{cases} \dot{x} = \frac{g^*}{Q(1-k)}[-\alpha * n(y) + z] \\ \dot{y} = \frac{g^*}{Qk}[(1-\alpha)\eta(y) + z] - Q_0(1-k)\, y \\ \dot{z} = -\frac{Qk(1-k)}{g^*}[x+y] - \frac{1}{Q}z \end{cases} \quad (2)$$

The parameters $\boldsymbol{n(y)}$, q, Q_0, k, and g are defined as:

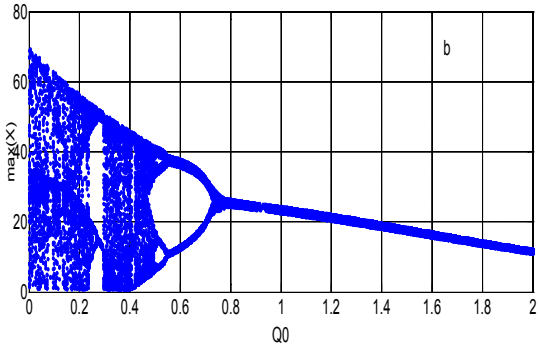
$$\begin{cases} n(y) = exp(-y) - 1 \\ k = \frac{C_2}{C_1+C_2} \\ Q_0 = G_0 w_0 \\ Q = \frac{w_0 L}{R} \\ g^* = \frac{LI_0}{(C_1+C_2)R_1 V_T} \end{cases} \quad (3)$$

A. *Bifurcation diagram for reel circuit*

In this part, we will analyze the bifurcation diagram of a real model and compare the results with the ideal model.



(a)



(b)

Fig.2 : bifurcation diagram real circuit :(a). As a function of the parameter g^*, (b) as a function of the parameter Q0

This diagram is obtained by plotting the maxima of the state x_2 as a function of the two parameters g and q_0 and all the other parameters are fixed. For the values of g^*=1.2; Q_0=0.8, the condition of Barkhaussen is satisfied and it presents the first sinusoidal oscillation. The first doubling of period will appear for g^*=2.7; Q_0=0.75.This bifurcation continuous to a critical value of g^*=3.6, Q_0=0.45 corresponding to the appearance of a chaotic behavior.

II. IDEAL MODEL

For $G_0 \to 0 \Rightarrow Q_0 \longrightarrow 0$, and $\alpha = 1$, the real model will be idealized and the number of parameters will be reduced, consequently, the analysis of the system will be simplified. In this case, the system depends only on g, this parameter allows a physical interpretation in terms of ideal model of oscillator, and mainly g defines the oscillation conditions and satisfies Criterion of Barkhausen [8]. We note that idealizing circuit does not affect the dynamics of the oscillator.

$$\begin{cases} \dot{x} = \frac{g^*}{Q(1-k)}[-n(y) + z] \\ \dot{y} = \frac{g^*}{Qk} z \\ \dot{z} = -\frac{Qk(1-k)}{g^*}[x+y] - \frac{1}{Q}z \end{cases} \quad (4)$$

A. *Bifurcation diagram for ideal circuit*

Figure. 3 shows the bifurcation diagram of the ideal circuit with g^* parameter dependence. For g^*=1.1 a sinusoidal oscillation is obtained corresponding to a limit cycle. When the value of g increases gradually, the changes have occurred at g^* = 2.6, g^*= 3.5 respectively. It is the transition from a two-period oscillation to a chaotic oscillation through period doublings.

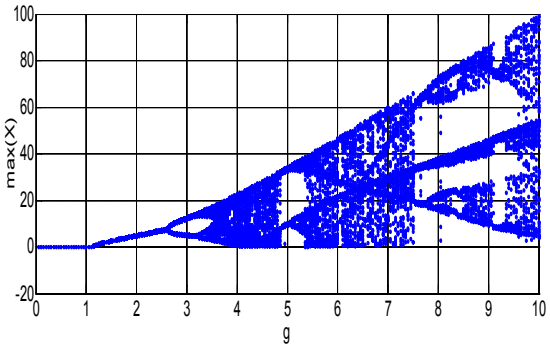


Fig.3. bigurcation diagram for ideal model

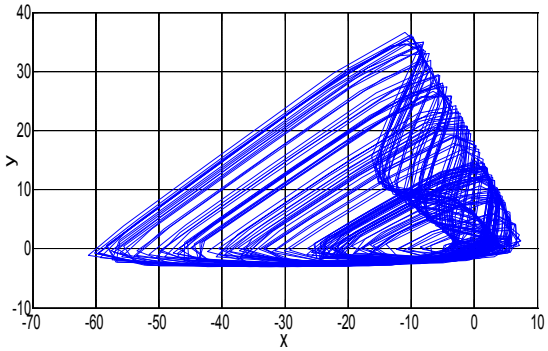


Fig 4. The phase space of colpitts oscillator

figure. 4 illustrates the phase space of ideal model for value of g * = 4.15, the strange atractor is obtained by plotting state y versus x of the system.

B. Simulation results

To improve control of current I0 we replace the current source with voltage source V2 and resistance R2 as shown in figure (5). The transistor used, is a bipolar transistor (BFP193) with f_T of 8GHz. The transistor is described in the simulations using a non linear ADS model.

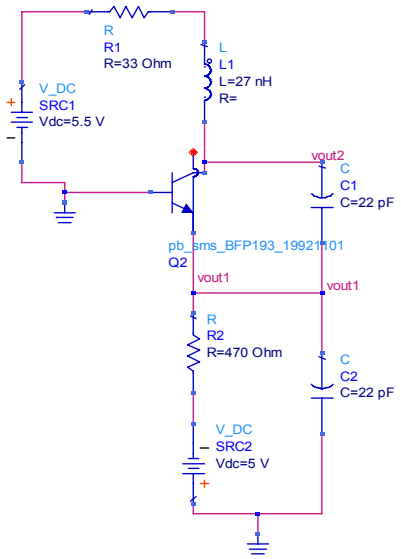
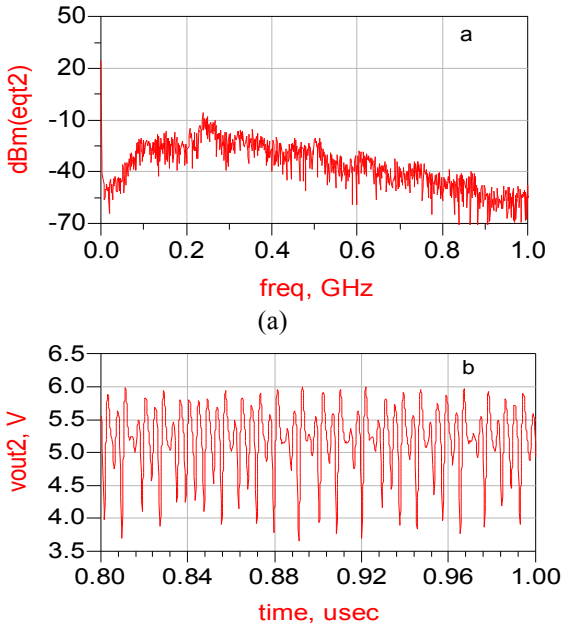


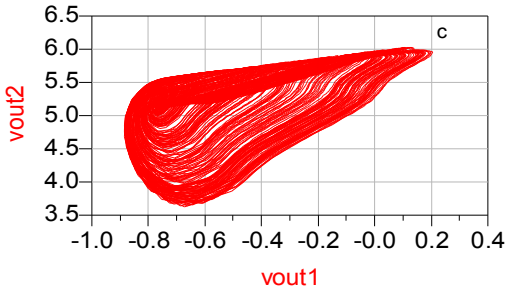
Fig.5.simulation circuit of colpitts oscillator.

The results of the simulations based on ADS model are shown by figure (6).



(a)

(b)



(c)

Fig.6. simulation results: (a) frequency spectrum (b) output voltage (c) the phase diagram of Colpitts oscillator

The elements of this circuit determines the fundamental frequency of the chaotic signal given by:

$$f_0 = \frac{1}{2\pi\sqrt{\frac{L_1 C_1 C_2}{C_1+C_2}}} = 292MHz \quad (5)$$

The frequency spectrum is reported in fig. 6. (a), it shows a spectrum up to 1 GHz with a large bandwidth of 600 MHz corresponding to different amplitudes (-50db to -10db). Fig.6. (b) shows the output signal of several V_{c2} as a function of the time and Fig.6. (c) shows the phase diagram of the oscillator: the output Vc_2 corresponds to the emitter base voltage of the transistor (V_{c2}=-Vbe) and Vc_1 corresponds to the collector emitter voltage (Vc_1=Vce).

IV. CONCLUSION

In this paper, we presented an analysis and comparaison of the bifurcation diagram for colpitts oscillator in both ideal and real circuits. This analysis reveals that the main difference between the two models remins on how the harmonic cycle is created . In other words, we can say that in the real model, the harmonic cycle incurs bifurcations similar to of the one in the ideal model with a slight difference in the value of the parameter g^*. Therefore, the analysis results of the simplified ideal Colpitts oscillator are also qualitatively valid for the actual model. On the other hand, the validity of our model is limited by the operating frequency, because when this later increases, the model should take into account another parameters of the transistor (such as the capacitis Cbe, Cce which will be included in parallel with C1 and C2 respectively)in order to have more accurate results.

REFERENCE

[1] L. O. Chua, “Chua's circuit 10 years later”. International Journal of Circuit Theory and Applications, Vol. 22, pp. 279-305. 1994

[2] M. P. Kennedy “Chaos in the colpitts oscillator”, IEEE Trans. Circuits and Systems, vol. 41, pp. 771–774. 1994

[3] Wenlan Chen, Shanwen Hu, Xiaozhou Liu, Haodong Wu, and G. P. Li “A non-common-node chaotic Colpitts oscillator with negative resistance enhancement”. IEICE Electronics Express, Vol.11, No.22, 1–6.2014

[4] W. L. Chen, L. H. Zheng and X. X. Song” Design of Two-stage Chaotic Colpitts Oscillator”. 978-1-4673-8983-9/16/$31.00. IEEE.2016

[5] Tamasevicius, G. Mykolaitis, S. Bumeliene, A. Cenys, A. N. Anagnostopoulos, and E. Lindberg” Two stage chaotic colpitts oscillator”. Electronics Letters, vol. 37, no. 9, pp. 549–551.2001

[6] Volkovskii, A. R. Tsimring, L. S. Rulkov, N. F. “Langmore, Spread spectrum communication system with chaotic frequency modulation”. American Institute of Physics, (Chaos), vol. 15, pp. 033101-1-6. 2005

[7] O.De Feo, G.M. Maggio, “Bifurcation in the Colpitts oscillator: from theory to practice” International Journal of Bifurcation and Chaos, Vol. 13, No. 10. 291-2934. 2002

[8] O.D. Feo, G.M. Maggio, M. P. Kennedy”The Colpitts oscillator: families of periodic solutions and their bifurcations” International Journal of Bifurcation and Chaos, Vol. 10, No. 5 935-958. 1999

[9] Chua, L. O., Desoer, C. A. & Kuh, E. S.Linear and Nonlinear Circuits (McGraw-Hill, NY).1987

Proposition of a New Vernam Chaotic Cipher

Hana ALI-PACHA - Naima HADJ-SAID – Adda ALI-PACHA*

Laboratoire **LACOSI** (Lab. de Codage et de la Sécurité de l'Information)

University of Sciences and Technology of Oran – Mohamed Boudiaf- USTO-MB, Algeria
Corresponding Authors, Email :{hana.alipacha, naima.hadjsaid}@univ-usto.dz, a.alipacha@gmail.com

Abstract :

The One Pad Time is the only encryption algorithm known to be undecipherable. It is actually a cipher with the characteristic that the encryption key has the same length as the plaintext message. This algorithm was hoping for a strong commercial success, but the problem of the size of the keys will be fatal to it, except for specific military applications, which require an irreproachable protection.

The fact that the key consists of a sequence of totally random characters is an essential condition for the security of the Vernam cipher (OPT). The surest way to respect this constraint is therefore to create the keys by exploiting the concept of insensitive sensitivity to the initial conditions of chaotic systems, which is a fundamental characteristic of dynamic systems.

In this paper, we will try to make a new reading of this algorithm and to try to find a practical solution to the size of this key by introducing the concept of chaos to this realization.

Key Words: One Pad Time, Vernam Cipher, Chaos, sensitivity to the initial conditions, Logistic Map

1. Introduction

The Vernam Cipher is based on the principle that each **plaintext** character from a message is 'mixed' with one character from a **key stream**. If a truly **random** key stream is used, the result will be a truly 'random' **ciphertext** which bears no relation to the original plaintext. In that case the cipher is similar to the unbreakable **One-Time Pad (OTP)** [1, 2, 3, 4]. Originally described in 1882 by banker Frank Miller (USA), it was re-invented in 1917 by Gilbert Vernam and Joseph Mauborgne. When applied correctly, the OTP provides a truely unbreakable cipher. It is named after the sheets of paper (pads) on which the key stream was usually printed. It also exists as *One Time Tape* (OTT).
As it was generally used with teleprinters and 5-level punched tape, the system is also known as One-Time Tape or OTT.

If the resulting **ciphertext** in the OTT system described above is truly random, it can safely be sent over the air, without the risk of being deciphered by an eavesdropper. All the recipient has to do is mix the ciphertext with the same OTT to reveal the original **plaintext**. One only has to guarantee that the OTT is truly random, that there are only two copies of it, that both copies are destroyed immediately after use and that they are only used once.

In this paper we will try to make a new reading of the **One-Time Pad** with the aim of solving the problem of the size and the hazard of this key. For that, we introduce the concept of chaos to this realization of these two objectives, but before proposing our New Vernam Chaotic Cipher in Section 4, we dedicate in Section 2 a study of chaos theory and attractors used in the rest of the paper. Section 3 describes the Vernam Cipher (**One-Time Pad OTP**), the last section concludes the paper.

2. Chaos Theory:

The chaos is generally defined [5, 6] as a particular behavior of a nonlinear deterministic and dynamical system. Mathematically, a dynamic system is defined from a set of variables that make up the state vector:

$$\mathbf{x} = \{x_i \in R\},\ i = 1...n \qquad (1)$$

Where *n* represent the dimension of the vector.

These sets of variables are the property to completely characterize the instantaneous state of the dynamic system generic. Associating in the more a coordinate system, we obtain the state space that is also called the phase space [5, 6].

It is a space of two or three dimensions in which each coordinate is a state variable of the system considered. Conjunction with state space a dynamic system is also defined by an evolution law, generally this dynamic characterizes the evolution of the system state in time.

A dynamical system is a typical system that evolves over time or in continuous (continuous time) described by differential equations which, however, are discretized for the purpose of computing: They are simulated by a time step very small compared to the scale time of the study phenomenon. Either discretely or in discrete time, they are the iterated applications.

An iterated application is a reduced description (in terms of information) of the system dynamics:

- The state of the system is described by a sequence of state vectors X_n, obtained by a Poincare section of the state space which belongs to the state vector X (t): in practice, the vector X

(t) is sampled at instants $t_n = n\,T$, which may for example be obtained by experimental measurements;

- The iterated application can then go from X_n state to X_{n+1} state, it can for example be constructed retrospectively from a large enough following vector X_n;

The interesting point is that the numerical simulation from the iterated application can bring back a resolution problem for a differential equation (non-linear) to problem significantly simpler, the equations with recurrences. In spite of reduction of information it requires on knowledge of the exact dynamics of the system, this simulation can nevertheless highlight a chaotic behavior, and the transition to chaos associated with it [5, 6].

A dynamic system usually has one or more parameters called "control", which act on the characteristics of the transition function. Depending on the value of the control parameter, the same initial conditions lead to trajectories corresponding to qualitatively different dynamical regimes. Changing the control parameter may lead to a change in the nature of dynamical regimes developed in the system.

The notion of determinism comes from the fact that a system is completely characterized by its initial state and its dynamics. A necessary condition for the appearance of chaos is that the system is non-linear. From an initial state x_0 (seed) and after a transitional regime, the trajectory of a dynamic system reaches a limited region of phase space. This asymptotic behavior obtained for t, k $\rightarrow \infty$ is one of the most important features [5] for any dynamic system.

2.1. Sensitivity to Initial Conditions

Sensitivity to initial conditions (S.I.C) is a fundamental characteristic [5, 6] of dynamic systems. Here means that a system will react completely differently depending on the initial condition (**Fig. 1d** and **Fig.2C**). This particular result in the fact of chaotic system, even if all its components are determined, is very unpredictable as sensitive to very small initial perturbations.

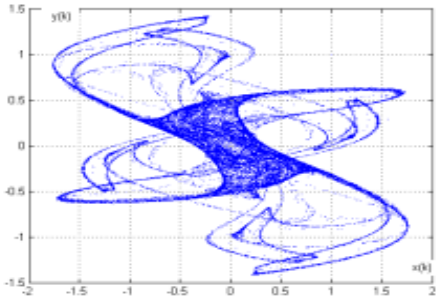


Fig.1a : Pickover's Attractor with 50000 iterations

2.2. Chaotic Attractor of Pickover

An example for an iterative application is the chaotic attractor of Pickover given by the system below.

$$\begin{cases} x_{k+1} = \sin(b.y_k) + c.sin(b.x_k) \\ \qquad\qquad j \\ y_{k+1} = \sin(a.x_k) + d.sin(a.y_k) \end{cases} \qquad (2)$$

For having chaotic behavior, Pickover chooses the values of the control parameters of the system as follows: a= -0.96, b=2.87, c=0.76, d=0.74. Figure 1a represents the Pickover's attractor for (x_0, y_0) = (1,1).

The evolution of *x(k)* and *y(k)* for this attractor and for the first 200 iterations are given by Figures 1b and 1c respectively.

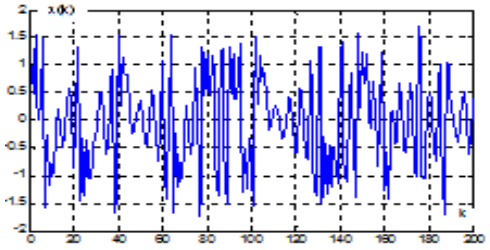


Fig.1b : Evolution of the signal *x(k)*

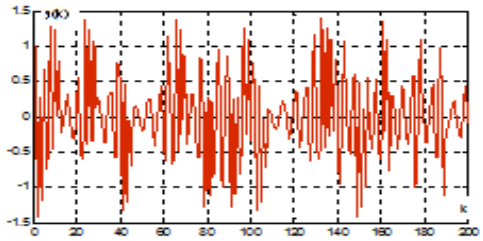


Fig.1c: Evolution of the signal *y(k)*.

We note that the two signals x(k) and y(k) are evolving in a chaotic way according of k, this behavior is accompanied by a high sensitivity to initial conditions as shown in Figure 1d (two signals x(k) and x'(k) are generated by two initial conditions of a difference of 10^{-10}):

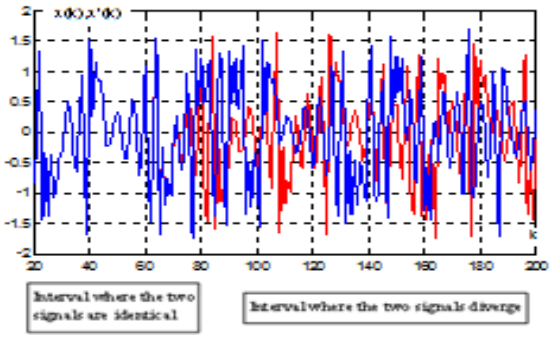


Fig.1d: Sensitivity of the attractor Pickover to initial conditions

We note that a very small error on the knowledge of the initial state (x_0, y_0) in the phase space will be rapidly amplified, and gives us two widely different signals. Quantitatively, the error growth is locally exponentially for strongly chaotic systems (sensitivity to initial conditions).

Note that the error on the initial conditions in this case is 10^{-15} and this is the smallest value for Matlab work with only 52 bits, but the system can be sensitive to values smaller than 10^{-15} according to the work environment.

2.3. Logistic Map

Logistics map [5, 6] is a well-known dynamic in non-linear systems theory, defined by equation (3):

$$y_{k+1} = r\, x_k\, (1-x_k) \qquad (3)$$

It gives a perfect explanation of a dynamic system behavior. This system was developed by Prof. Pierre François Verhulst (1845) to measure the evolution of a population in limited environment, later used in 1976 by the biologist Robert May to study the evolution of insect population:

- y_{k+1}: Generation in the future that is proportional to x_k.
- x_k: Previous generation.
- r: Positive constant incorporates all factors related to reproductive, successful overwintering eggs for example, etc.

In order to study this dynamic system and some asymptotic individuals' models, the first thing to do is to draw the parabolic graph $y= r.x\ (1-x)$, and the diagonal $y=x$.
The operation that we will follow to draw the iterative form y_{k+1} according to x_k is simply summarized as following:

- Starting from an initial value x_0 of the x-axis, we reach the function with a vertical; the function takes the value $y_1=r.x_0\ (1-x_0)$,
- From horizontal $y_1= r.x_0\ (1-x_0)$ of the previous point, we join the line $y = x$;
- We represent the abscissa of the intersection with the vertical line $x=x_0$; we have $y_1 = x_1$
- From the x_1 value of the x-axis, we reach the function with a vertical; the function takes the value $y_2= r.x_1\ (1-x_1)$; and so on.

We take $r = 3.9$ and, $x_0=0.01$ for logistics map, the previous operations for 100 iterations are represented in Figure 2a.

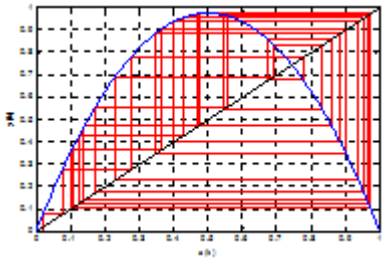


Figure 2a. Evolution of y_k in function of x_k

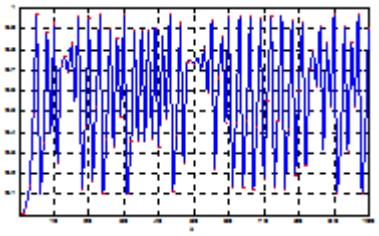


Figure 2b. Chaotic regime in function of k

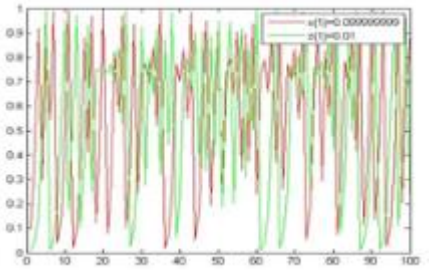


Figure 2c. Sensitivity to initial conditions

3. Vernam Cipher: One-Time Pad (OTP)

Although simple, easy and fast, for both coding and decoding, this encryption is the only one that is theoretically impossible to break, even if it presents significant difficulties in practical implementation. The magazine Sciences et Avenir of September 2011, p.27, indicates that "as early as 1882, the American banker Frank Miller laid the foundations". It is currently used by states. Indeed, they can communicate the keys to their embassies in a safe way via the diplomatic bag. It would have been used by Americans and Russians to encrypt the communications of the famous "red phone".

3.1 Principle

The encryption by the Vernam Cipher consists in combining the plaintext message with a key having the following very particular characteristics:

1. The key must be a sequence of characters at least as long as the message to be encrypted.

2. The characters making up the key must be chosen in a totally random way.

3. Each key, or "mask", should only be used once (hence the name of the disposable mask).

The combination method between plaintext and key is simple and will be described below.

Alice wants to send Bob a message M. Using the secret key K (agreed with B), it will encrypt M to arrive at its encrypted version C. Let's write:

$$C = K * M \qquad (4b)$$

Where "*" is a group algebra [7, 8, 9]. The use of a group law is justified because it has a necessary property:

*Whatever two numbers a and b, there exists a unique number x such that a = b * x*

The reverse operation of the one that allowed the encryption is used:

$$M = K (*)^{-1} C \qquad (4b)$$

In general, il used Fields of Galois $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z} =$ field with p elements, p a prime number.

It is symbolizing by modulo 2, and is denoted by XOR. The symbol ⊕ is used:

a	b	C=a⊕b
0	0	0
0	1	1
1	0	1
1	1	0

In this case, the encryption is done by adding the key to the message modulo 2, bit by bit. This process is often called exclusive.

However, in practice, we use modulo (256). The value of 256 represents the number of characters used in the ASCII code if, the message to be encrypted is a text, also represents the number of colors in a BMB extension image if, the plaintext is an image.

In this case, we use a specific group algebra "*" as {Z/256Z, +} a set of numbers modulo 256. Let we have a generator produces a stream of known length of numbers modulo 256 (streamkeys): K_1, K_2, K_3, ..., K_i ... with certain properties of chance, it is potentially difficult to identify the groups of numbers following a certain rule (group behavior). The output of such a generator is not completely random, but only they approached to the ideal properties of completely random sources. It is said random because this sequence is arbitrary. This stream is combined with exor function to the bit stream of the plaintext m_1, m_2, m_3, …, m_i; to produce the bit stream of encrypted data.

$$C_i = m_i + K_i \bmod(256) \qquad (5a)$$

Sides of decipherment, the encrypted data bits are oxored, with a stream data identical to a process's cipher to retrieve bits of plaintext:

$$m_i = (C_i - K_i) \bmod(256) = \qquad (5b)$$

$$(((m_i + K_i) \bmod(256) - K_i) \bmod(256) = \qquad (5c)$$

$$(((m_i + K_i) - K_i) \bmod(256) = \qquad (5d)$$

$$((m_i + K_i - K_i) \bmod(256) = m_i \bmod(256) = m_i \qquad (5e)$$

The Vernam cipher follows the principle detailed above:

• An alphabet E={Z/256Z, +}, on which are written the messages in clear and the encrypted messages

• 256 the number of letters of E (256 = #E)

A message M of n symbols M = (x_1, x_2, ..., x_n) is expressed by the transformation fK:

f_K: M (x_1, x_2, ..., x_n) -> C ($_{y1}$, y_2, ..., y_n)

where $y_i = x_i + k_i \bmod 256$

with K = (k_i, ..., k_n) the key chosen randomly in E, and destined to serve only once.

3.2 Problem of Using a Single and Unique Key

That is, a message M_1 masked by the key K, we get the cipher C_1. Suppose another message M_2 is encrypted with the same mask K, providing the cipher C_2. Let us agree that the symbol ⊕ here represents the application of the XOR operation to each of the bits. We have the following relationships:

$$C_1 = M_1 \oplus K \qquad C_2 = M_2 \oplus K$$

Suppose an opponent applies the XOR operation to both C_1 and C_2, and re-uses the properties seen above:

$$(C_1 \oplus C_2) = (M_1 \oplus K) \oplus (M_2 \oplus K) =$$

$$(M_1 \oplus M_2) \oplus (K \oplus K) = (M_1 \oplus M_2)$$

We obtain the XOR of the two-plaintext messages. This is very dangerous because any mask effect of key K has disappeared. If, for example, an adversary knows the two encrypted messages or one of the plaintext message, he can instantly find the second plaintext message by the calculation:

$$C_1 \oplus C_2 \oplus M_1 = M_2$$

In fact, even without knowing one of plaintext message, more complex methods can often to find M_1 and M_2.

In practice, the safe use of the disposable mask requires a rigorous organization, each key must be precisely identified and carefully traced, especially since it is always provided in two copies, two correspondents geographically distant. Imagine that a Chancery communicates through this method with its dozens of embassies in countries of the world, each of them sending and receiving several messages a day, which can include a large number of pages, and this for years: it takes heavy logistics to guarantee absolute security, and what we want to solve in this work.

3.3"Unconditional" security

If the chosen key is subject to the conditions mentioned above, the use of a group law (⊕) guarantees so-called unconditional security. Indeed, if we accept that a cryptanalyst intercepts the encrypted message C, he can not deduce anything from it, except the size of the plaintext message M. It is impossible for him to establish a correlation between M and C without to know K, because since we use to enforce a group law, for M and C there exists only one number K such that:

$$M = K * C !$$

4. Vernam Chaotic Cipher

We summarize the disadvantages related to the One Time Pad, which will be taken into account to realize our own crypto system, and which are:

1. Problem of the length of the key and the generation of keys randomly.
2. Numbers of keys required, because we also work often with several correspondents, each having several sets of keys in common,
3. Guarantee the unique use of each key, even years apart,
4. Problem of their transmission to the correspondent, of their storage, of their identification.

All of these points pose significant organizational problems if not; the security of the system may be compromised. To remedy this, we resort to chaos theory.
The proposed cryptosystem is the Vernam Chaotic Cipher is a secret key system. The same steps of the VCC system are used in encryption and decryption. The novelty of this system is the generation of the key.

4.1 Production of a Perfectly Random Key

Let N be the total number of characters of the message to be encrypted. Let's give two numbers P and Q such that:

$$P * Q \geq N$$

N, P and Q are numbers used in the constitution of the key fields.
To fill this matrix, we roll out firstly the Pickover's attractor, which is 2-dimensional which gives us a couple (x, y) of values, this couple will be transformed by the following relation:

$$(x, y) \rightarrow (x*H \text{ modulo } P, y*H \text{ modulo } Q)$$

To give us a box in the matrix predicted above.

H is a constant number of the order of 10^9 in order to amplify the amplitudes of the Pickover's attractor.

H is also part of the key field.

Once one box of matrix is chosen, we unfold the algorithm of the logistics map to give us a value z, we transform this value by the following relation:

$$z \rightarrow z*H \text{ modulo } 256$$

To obtain a value between 0 and 255. This result, is assigned to the chosen box.

We start the process to choose, by the Pickover's attractor, another box not filled, to fill it via the logistics map.

Once the matrix is filled, the mask of the message to be encrypted is constituted by reading the cells of the matrix line by line up to the number N of cells of the matrix to be xorated with the plaintext message.

✓ We propose the following chart, figure 3:

Initial conditions:

1) For the Pickover attractor: The fixed values a= -0.96, b=2.87, c=0.76, d=0.74 and we take $x_0 = 1$ and $y_0 = 1$ as the variables values.
2) For the logistic map: The fixed value is r = 3.9 according to the equation z_n, we take $z_0 = 0.1$ as the variable value.
3) Starting values N1|N2 (see figure 4) respectively for Pickover attractor and logistics map are 37 and 53.

For i = 1 to P
  For j = 1 to Q
    $h \rightarrow Line = mod(fix(x_n*H), P)$
    $k \rightarrow Column = mod(fix(y_n*H), Q)$
    $M(h, k) = mod(fix(z_n*H, 256)$
End, end.

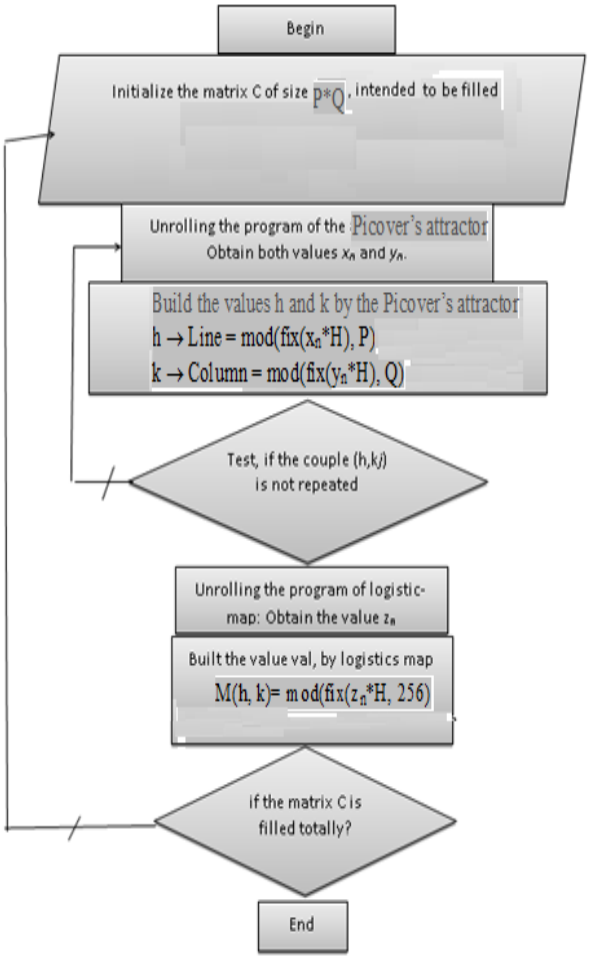


Figure 3. Chart of key construction

In conclusion, we have resolved the Problem of the length of the key and the generation of keys randomly. The Numbers of keys required of several correspondents, each having several sets of keys in common is resolved by choosing different couple of P and Q.

The problem of distribution or storage of a key is a common problem of .all rather secrete cryptosystem. We still have, the third drawback that will be dealt with in the next paragraph.

4.2 Guarantee the unique use of each key

We will exploit the sensitivity to the initial conditions of the systems to guarantee the uniqueness of the key.

Let have the folowing values:

$X_{0,1}$=0.1
$X_{0,2}$=0.100310100065779
μ_1= 3.9
μ_2= 3.900110520190021 54
H= 10^7.
N= 70000

If, I assume that in (μ_2 and distributed in this way) that on, May 11, 2019 at 21h 54m, I sent an encrypted message.

Also, we assume that in ($X_{0,2}$ and distributed in this way) that we have send a message for two different corresponds of registration number 3101 and 65779.

We take 4 different suites, each one of 70000 values, from the logistics map and, for different initial conditions.

	$X_{0,1}$	$X_{0,2}$	μ_1	μ_2
U(n)	X		X	
V(n)		X	X	
W(n)	X			X
T(n)		X		X

n	U(n)	V(n)	W(n)	T(n)
1	64	64	64	64
2	240	240	240	240
3	193	193	193	193
4	72	72	72	72
5	128	128	128	128
6	115	115	115	115
7	204	204	204	204
8	155	155	155	155
9	210	210	210	211
10	158	158	158	158
11	140	140	140	140
12	105	105	105	105
13	119	119	118	118
14	4	4	3	3
15	151	151	154	154
16	128	128	134	134
17	155	154	145	145
18	22	23	45	46
19	198	197	182	181
20	52	54	108	110
21	203	208	75	81
22	125	119	242	236
23	139	158	60	79
24	191	213	182	204
25	253	187	8	198
26	158	99	79	20
27	118	56	6	201
28	252	85	3	91
29	87	118	206	235
30	231	248	104	113
31	207	203	181	180
32	89	193	133	94
33	171	43	235	125

Figure 4. 4 sequences values

The table in Figure 4 represents the 4 data sequences from the logistics map with initial conditions very close.

Note that from a given threshold (n = 24), the values of these 4 sequences are different. This is due to the influence of the characteristic of the sensitivity to the initial conditions of the logistics map.

4.2.1. Frequency Test

The most natural test is that of the frequencies of occurrence of each digit, for a real random sequence, a particular number has no reason to be more or less represented than another. In other words, the frequencies of each digit must eventually come close to 10%. Obviously, the same thing is expected from our pseudo-random generator: this is the first test to which it is subjected.

It can be seen in the graph of figure (5) that all the values from 0 to 255 are represented approximately with the same frequency of occurrence. This gives that the generator of T(n) passes this test.

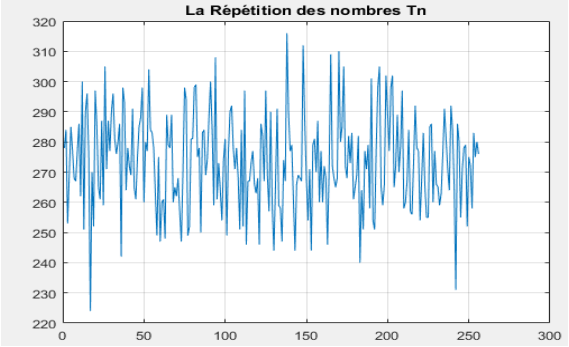


Figure 5. Frequency Test of Numbers

4.2.2 Entropy

Shannon entropy is a mathematical function that intuitively corresponds to the amount of information contained or delivered by a source of information. For a source, which is a discrete random variable X comprising n symbols, each symbol x_i having a probability P_i to appear, the entropy H of the source X is defined as:

$$H(x) = -\sum_{i=1}^{n} P_i . log_2 (P_i) \qquad (6a)$$

We pose

$$P_i = \frac{k_i}{n} \qquad (6b)$$

The entropy of the sequence T(N) is: **7.9979 bits**

On the other hand, consider a source that has an alphabet of 256 characters. If all these characters are equiprobable, the entropy associated with each character is **$\log_2(256) = \log_2(2^8) = 8$ bits**, which means that it takes 8 bits to transmit a character thus, its entropy is equal to **8 bits**.

Nature of Source	Entropy in bits/symbols
Source of T(n)	**7.9979**
Source that delivers equiprobable characters	**8**

There is a ratio that the source of T(n), is 99.97% of a source that delivers equiprobable characters. Therefore, our generator passes the entropy test.

4.2.3.Mean, Variance and autocorrelation factor Tests

We must test the distribution of the numbers produced in the sequence in its interval of operation, we have calculated the three operators: the mean, the variance and the autocorrelation function of these numbers, the results obtained figure (6) are close to the ideal case results.

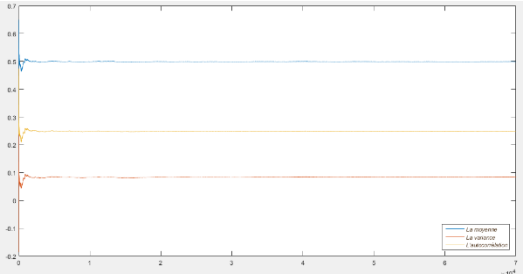


Fig.6: Mean, Variance and autocorrelation factor Tests

The figure (6) confirms us that, the numbers generated by T(n), have a random behavior.

4.2.4. Spectral analysis

Knuth [10, 11] describes the spectral test as the most discriminating of all. Indeed, no proven bad generator could succeed. Very simple, the method consists in studying the distribution of the values generated in a dimension k (2D or 3D) to check the quality. In fact, all LCG generators suffer from a Marsaglia effect (this is because we do not generate all the real numbers, but only fractions are generated).

- **Dimension2 (2D):** Two consecutive values will be the coordinates of a point on the plane, figure 7. One looks if; the points are uniformly distributed in a square.

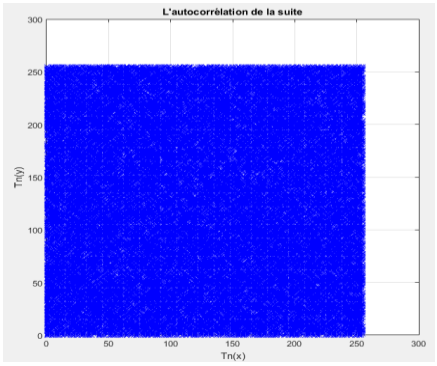


Fig.7: Spectral Test of dimension 2D.

Therefore, the smaller the inter-planar distance, the better the generator.

- **Dimension 3 (3D):** Three consecutive values will be the coordinates of a point in space. One looks if; the points are distributed evenly in a cube. By turning the cube, one sees the undesirable effect: plans of Marsaglia. It can be seen below that the points are located on planes.

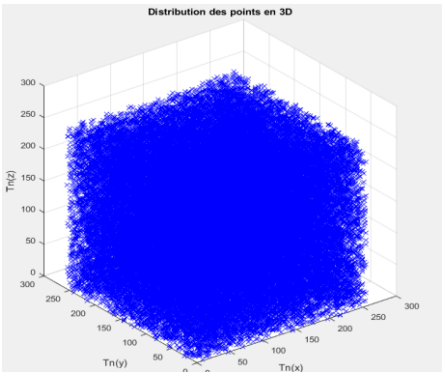


Fig.8: Spectral Test of dimension 3D

In general, the spectral test makes it possible to determine the deviation d between two lines. At the most, this gap is small at most the generator is of good quality. We find that the generator of equation T(n) succeed this spectral test.

4.3 Fields of the Key or Mask

In the proposed algorithm, the secret key field is set as follows:

N	P	Q	M_1	M_2	H	X	Y	Z

Initial state of the logistics map z_0=0.1, and Pickover's attractor x_0=1, y_0=1, H=10^7, the encryption key can be represented by the following fields:

- ✓ x_0, y_0, z_0,
- ✓ F : scalar≈ 10^7.
- ✓ M_1 and M_2 : starting point or the starting moment k, where we begin to do the encryption.
- ✓ N: size of characters message ≈ 10^7
- ✓ P≈Q≈10^4

Where x_0, y_0, z_0 are double precision numbers. N, P, Q and M_1 and M_2 are integer constants. If the precision of calculating x_0, , y_0, z_0 is 10^{-16}, and $M_1|M_2 \in$ [1, 1000].

Therefore, the key space is larger than

$\approx 10^{16}x10^{16}x10^{16}x10^{7}x\ 10^{7}\ x\ 10^{4}\ x\ 10^{4}\ x\ 10^{3}\ x\ 10^{3}=10^{76}$

(with $10^3 \approx 2^{10}$) in this case we will have a key field of the order of 2^{228}.

We have 228 bits larger of key.

4.4 Example of the Encryption

Let be the dat key a of section 4.2, let the Lena BMP image to be encrypt.

The folowing result is found:

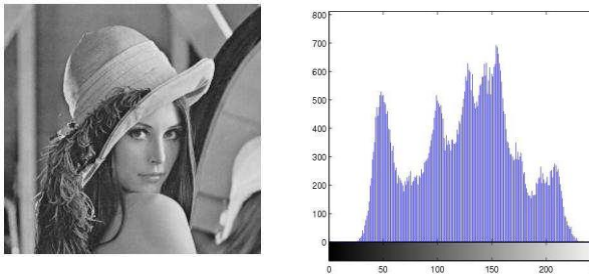


Figure 9a. Image of Lena in plaintext and its histogram

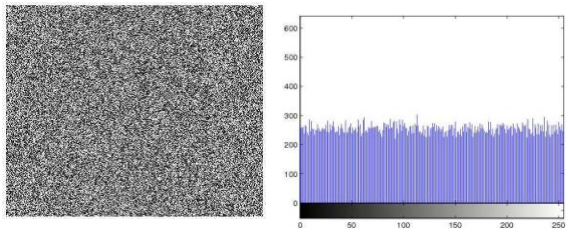


Figure 9b. Image Lena encrypted and its histogram

Referring to the results obtained, we can clearly see that the simple image differs significantly from the corresponding encrypted. Moreover, the histogram of the encrypted image is fairly uniform which makes it difficult to extract the statistical nature of the simple image pixels. Histograms of plaintext and encrypted images of Lena showing that our Vernam Chaotic Cipher works correctly.

One found the following values for the entropy of plaintext image of Lena is (7.4651) and for her encrypted image is equal to (7.9987).

It is found that the entropy of the images increases to almost 8 bits (99.98% of ideal case; see section 4.2.2) showing that encryption creates a high level of disorder.

5. Conclusion

One realized a new Vernam system based on chaotic attractors.

The advantage of this proposal is the reduction of the key (228 bits) for a message of 70000 characters.

the key found is doubly random, because after creation through the logistic map of this key, we made a permutation of order within the sequence of characters of this key.

In addition, we have 228 bits larger of key, this number is huge. Therefore, the encryption algorithm has a very large key space to withstand all kinds of brute force attacks.

References

[1] Schneier, B., (1996), " Applied Cryptography-Protocols, Algorithms and Source Code in C", John Wiley & Sounds, Inc, New York, Second Edition, 1996.

[2] A. J. Menezes, P. C. V. Oorschot, S. A. Vanstone, " Handbook of applied cryptography" 1997 by CRC Press LLC.

[3] https://www.cryptomuseum.com/crypto /vernam.htm

[4] Dirk Rijmenants, Secure Communications with the One Time Pad Cipher, Paper (English) 2009-2014. Version 6.2, 18 December 2014.

[5] Devaney, L. (1992) A First Course in Chaotic Dynamical Systems, Westview Press (Oct. 21st, 1992), Edition, 321 pages, Studies in Nonlinearity, ISBN: 9780813345475.

[6] Gleick, J. (1987) "Chaos: Making a New Science", Albin Michel edition, 420 pages,

[7] Jeffrey Hoffstein, Jill Pipher, J.H. Silverman, "An Introduction to Mathematical Cryptography", 524 pages, Springer-Verlag New York, 2008.

[8] Alfred J. Menezes, Paul C. van Oorschot, Scott A. Vanstone, "HANDBOOK of APPLIED CRYPTOGRAPHY", 794 pages, CRC Press, Taylor & Francis Group, 1996

[9] Chuck Easttom, "Modern Cryptography: Applied Mathematics for Encryption and Information Security", 505 pages, McGraw-Hill Education, 2016

[10] Knuth, D.E., (1998), "The Art of Computer Programming", Addison-Wesley, Reading, MA, third edition, 1998.

[11] Chen G. & Mao,Y. & Chui, C. K., (2004), "A symmetric image encryption scheme based on 3D chaotic cat maps", doi:10.1016/j.chaos.2003.12.022, Chaos, Solitons and Fractals 21, pp: 749–761, 2004.

Efficient FPGA Implementation of Modular Multiplication and Exponentiation

M. Issad
Centre de Développement des Technologies Avancées, CDTA
Baba Hassen, Alger, Algérie
missad@cdta.dz

M. Anane
Ecole Supérieur d'Informatique, ESI,
Oued Smar, Alger, Algerie
m_anane@esi.dz

B. Boudraa
Université des Sciences et de la Technologie Houari Boumediene,
Bab Ezzouar, Alger, Algerie
b.boudraa@yahoo.fr

A. M. Bellemou
Centre de Développement des Technologies Avancées, CDTA
Baba Hassen, Alger, Algérie
abellemou@cdta.dz

N. Anane
Centre de Développement des Technologies Avancées, CDTA
Alger, Algerie
anane@cdta.dz

***Abstract*— This paper presents an FPGA implementation of the most critical operations of Public Key Cryptography (PKC), namely the Modular Exponentiation (ME) and the Modular Multiplication (MM). Both operations are integrated in Hardware (HW) as Programmable System on Chip (PSoC). The processor Microblaze of Xilinx is used for flexibility. Our objective is to achieve a best trade-off between execution time, occupied area and flexibility. In order to satisfy this constraint, Montgomery Power Ladder and Montgomery Modular Multiplication (MMM) algorithms are utilized for the ME and for the MM implementations as HW accelerators, respectively. Our implementation approach is based on the digit-serial method for performing the basic arithmetic operations. Efficient parallel and pipeline strategies are developed at the digit level for the optimization of the execution time. The application for 1024-bits data length shows that the MMM run in 6.24 µs and requires 647 slices. The ME is executed in 6.75 ms, using 2881 slices.**

Index Terms— Modular Exponentiation, Montgomery Modular Multiplication, PKC, FPGA.

I. INTRODUCTION

Modular Exponentiation (ME) over Galois field GF(M) is a common operation used in several Public Key Cryptography (PKC), such as Diffie-Hellman key exchange scheme [1], Rivest, Shamir and Adleman (RSA) cryptosystem [2] and Digital Signature Algorithm (DSA) [3]. At low abstraction level of ME, the computation complexity is reduced to intensive execution of the Modular Multiplication (MM) on large integers. This operation could be performed by a multiplication followed by a division. However, in literature several algorithms were developed in order to avoid the division, as this latter is a costly operation [4]. Among these algorithms, Montgomery Modular Multiplication (MMM) is the most popular algorithm used to speed up the MM execution [5]. This method transforms the modular reduction to a series of additions and right shifts.

In this paper, FPGA implementation of the ME over GF(M) is presented, based on the combination of the MMM and of the Montgomery Power Ladder (MPL) algorithms [6]. Our main objective is to find a best trade-off between flexibility, execution time and occupied area for the hardware implementation of the MMM and for the Hardware/Software (HW/SW) co-design of the ME. The proposed work is a Programmable System on Chip (PSoC) where the soft processor core Microblaze of Xilinx [7] is used for flexibility.

In this work, our challenge consists in the design of a flexible ME co-processor which can be easily adapted to different PKC schemes. Indeed, the flexibility criterion is an important factor which provides a possibility for updating system functionalities without modifying the hardware architecture. In PKC, modifications and updates are generally related to system security level or to target application. For RSA or DSA designs, security is provided by the parameters defining the modulus and the exponent sizes used for computing the ME.

In order to ensure the system flexibility, our first contribution consists in the proposed HW/SW partitioning for managing the modulus, the exponent and their sizes. The implemented ME co-processor is based on the definition of the modulus and the exponent sizes in SW. In addition, registers and data memory are integrated within the architecture of the ME coprocessor. These components are re-sized according to the security level parameters.

The other criteria focused in our work concerns the achievement of the best trade-off between the execution time and the requirement of hardware resources. Indeed, when long integers are used, the MMM algorithm needs not only long carry propagation paths and large multipliers but also, long registers. In order to speed up the MMM execution, parallel and pipeline techniques based on systolic architectures [8], [9] redundant number systems [10] and carry save adders [11] are often used. Although these methods lead a high throughput, the corresponding architectures require more resources and are not suitable for the design that we target. Unlike to these works, the constraints considered in our MMM implementation are related to : (i) the data bus should be independent and very small compared to the inputs data length; (ii) the scalability of the design to support any operand length; (iii) the adaptation between the ME execution and the data bus of the used embedded processor. Thus, in order to satisfy the considered

criteria, our second contribution consists in the implementation of an optimized Montgomery Modular Multiplier (*MMMulr*). This latter is applied then for the HW/SW co-design of the ME co-processor.

The rest of this paper is organized as follows: Section II describes the background of the MM and of the ME algorithms. Section III details the MMM digit-serial algorithm. Section IV presents the FPGA methodology of the MMM and of the ME co-processor designs. Section V discusses the obtained experimental results and comparisons with previous implementations. The conclusion is given in section VI.

II. Background and Algorithms

In this section, we start our description by an overview of the MMM. Then, the computation of the ME based on the combination of the MMM with the MPL algorithm is presented.

A. Montgomery Modular Multiplication

Let A, B and M three integers where $0 \leq A, B < M$ and M is odd of $m - bits$ size. Instead of performing the division by M to compute $(A \times B)\ mod\ M$, Montgomery proposes to transform the required operation to a trivial division by R where R is a power of 2, chosen such that: $R \geq 2^m$ and $gcd\ (M, R) = 1$ [5].

Montgomery modular multiplication is defined by the following equation:

$$S = (A \times B \times R^{-1})\ mod\ M \quad (1)$$

Using equation (1), the MMM result (S) is obtained with an additional factor R^{-1}. To remove this latter, the method requires the conversion of A and B to the Montgomery domain. Then, the expression (1) is performed on the new operands, obtained from the first step. Finally, the result is recovered in the classical domain.

B. Modular Exponentiation Algorithm

In our work, MPL algorithm is used for the ME implementation. Its execution process uses the binary expansion of the exponent E, scanned bit-by-bit from left to right. At each iteration, modular squaring and MM are performed in parallel [6]. The MPL algorithm combined with the MMM is given as follows:

Algorithm 1. Montgomey Power Ladder Algorithm

Inputs: X , **M and E with** $\mathbf{E} = \sum_{i=0}^{t-1} e_{(i)} \times 2^i$
Pre-computed: R^2 mod M, **with** $R = 2^{(n+1)\times k}$
Intermediate variables: $\mathbf{R0_{(i)}}$, $\mathbf{R1_{(i)}}$
Output: Y $= X^E$ mod M
Begin
1. $R0_{(t)} =$ Mont (1, R^2 mod M)
2. $R1_{(t)} =$ Mont (X, R^2 mod M)
3. for i **from** t-1 **to** 0 **do**
4. **If** $\mathbf{e_{(i)} = 0}$ **then**
5. $R0_{(i)} =$ Mont ($R0_{(i+1)}$, $R0_{(i+1)}$)
6. $R1_{(i)} =$ Mont ($R0_{(i+1)}$, $R1_{(i+1)}$)
7. **else**
8. $R0_{(i)} =$ Mont ($R0_{(i+1)}$, $R1_{(i+1)}$)
9. $R1_{(i)} =$ Mont ($R1_{(i+1)}$, $R1_{(i+1)}$)
10. end for
11. Y=Mont ($R0_{(0)}$, 1)
12. Return Y

In this algorithm, $Mont(.)$ denotes the Montgomery function. It allows the computation of the required MMMs operations.

The combination of MMM and MPL algorithm for the ME computation, uses an initialization at the beginning of the execution process. This step is defined by the lines (1) and (2). It corresponds to the conversion of 1 and X to the Montgomery domain, respectively. Then, the iterative process executes the MPL algorithm from line 3 to line 10. The result $R0_{(0)} = (X^E \times R)\ mod\ M$ obtained at the iteration $i = 0$ is converted to the classical representation by using the MMM of line 11. This last is execute using $R0_{(0)}$ and $'1'$ as operands such that:

$$Y = [((X^E \times R)\ mod\ M) \times 1 \times R^{-1}]\ mod\ M = X^E\ mod\ M \quad (2)$$

The Complexity computation $CcMpl(t)$ of MPL algorithm depends not only on the exponent size, but also on the execution performances of MMM. $CcMpl$ is evaluated by expression (3).

$$CcMpl\ (t) = (t + 2)\ MMMs \quad (3)$$

The complexity $CcMpl\ (t)$ shows that the MMM plays a crucial role at the low abstraction level. Therefore, the optimization of this operation is an important step in the implementation process of the ME. In our case, the suitable improvements are related to the HW/SW co-design approach, based on a PSoC environment. The efficient method to implement this operation in such platform is to use the MMM digit-serial algorithm which provides both: adaptation of the MMM execution to Microblaze data bus and reduction of the hardware resources number.

III. MMM Digit-Serial Algorithm

Our work is based on the Finely Integrated Operand Scanning (FIOS) method which is digit-serial algorithm [12]. This latter is considered as a modified high radix MMM algorithm, where inputs and output are coded $n + 1$ digits of $k - bits$. 2^k becomes the used radix for representing the data and executing the basic arithmetic operations. For the FPGA implementation, we exploit the DSP48E cores to realize $k \times k - bits$ multipliers. Instead of long registers, the $18kbits$ blocks RAM are used to store the data. Furthermore, to adapt the MMM execution to the processor resources, the choice of the parameter k value corresponds to the data path size of the processor. As we use Microblaze which is a $32 - bits$ soft core, the value of k is set to 32.

A. FIOS-Modified High Radix MMM Algorithm

The FIOS-modified high $radix - r$ $(r = 2^{32})$ MMM algorithm without final subtraction is given as follows:

Algorithm 2. FIOS-modified high radix MMM algorithm

Inputs : $A = \sum_{i=0}^{n} A[i] \times 2^{i\times 32}$, $B = \sum_{j=0}^{n} B[j] \times 2^{j\times 32}$,
$M = \sum_{j=0}^{n} M[j] \times 2^{j\times 32}$ with $M[n] = 0$
Pre-computed: $M' = -M[0]^{-1} \bmod 2^{32}$, $R = 2^{(n+1)\times 32}$ **with** gcd (M, R)=1.
Intermediate variables: $S_{(i+1)} = \sum_{j=0}^{n} S[j]_{(i+1)} \times 2^{j\times 32}$,
$P1_{(i)} = \sum_{j=0}^{n} P1[j]_{(i)} \times 2^{j\times 32}$, $C1 = \sum_{j=0}^{n} C1[j]_{(i)} \times 2^{j\times 32}$,
$U_{(i)} = \sum_{j=0}^{n+1} U[j]_{(i)} \times 2^{j\times 32}$,
$P2_{(i)} = \sum_{j=0}^{n} P2[j]_{(i)} \times 2^{j\times 32}$, $C2 = \sum_{j=0}^{n} C2[j]_{(i)} \times 2^{j\times 32}$,
$Z_{(i)} = \sum_{j=0}^{n+1} Z[j]_{(i)} \times 2^{j\times 32}$, $c_1^j, c_2^j, c_3^j, c_4^j$

Output: $S = \sum_{j=0}^{n} S[j]_{(n+1)} \times 2^{j \times 32} = (A \times B \times R^{-1}) \bmod M$

Begin

1. $S_{(0)} = 0$

2. **for** i **from** 0 **to** n **do**

3. $P1[0]_{(i)} = A[i] \times B[0]$

4. $U[0]_{(i)} = P1[0]_{(i)} + S[0]_{(i)}$

5. $q_{(i)} = (U[0]_{(i)} \times M') \bmod 2^{32}$

6. $C1[-1]_{(i)} = C2[-1]_{(i)} = 0$

7. $c_1^{-1} = c_2^{-1} = c_3^{-1} = c_4^{-1} = 0$

8. **for** j **from** 0 **to** n **do**

9. $(C1[j]_{(i)}, P1[j]_{(i)}) = A[i] \times B[j]$

10 $(c_2^j 2^{32}, c_1^j 2^{32}, U[j]_{(i)}) = P1[j]_{(i)} + C1[j-1]_{(i)} + S[j]_{(i)} + c_1^{j-1} + c_2^{j-1}$

11. $(C2[j]_{(i)}, P2[j]_{(i)}) = q_{(i)} \times M[j]$

12. $(c_4^j 2^{32}, c_3^j 2^{32}, Z[j]_{(i)}) = U[j]_{(i)} + P2[j]_{(i)} + C2[j-1]_{(i)} + c_3^{j-1} + c_4^{j-1}$

13. $S[j-1]_{(i+1)} = Z[j]_{(i)}$

14. **end for**

15. $U[n+1]_{(i)} = C1[n]_{(i)} + c_1^n + c_2^n$

16. $Z[n+1]_{(i)} = U[n+1]_{(i)} + c_3^n + c_4^n$

17. $S[n]_{(i+1)} = Z[n+1]_{(i)}$

18. **end for**

19. Return $S = S_{(n+1)}$

The execution process of this algorithm is detailed in [13]. The computation complexity $CcMMM$ of this latter for performing the MMM is evaluated by:

$$CcMMM = (n+2) \times (n+1) \quad (4)$$

In this equation, the terms $(n+1)$ and $(n+2)$ correspond respectively to the size of operand A and of the cycles count required for the execution of the inner loop, respectively.

B. MMM Digit-Serial Algorithm Based on Parallel Execution Approach

The digit-serial approach for computing the MMM can be performance limited, since the MMM algorithm is executed in serial mode. In order to increase the MMM timing performances, we introduce a parallel execution mode, based on a pipeline scheme for performing the algorithm 2; while leaving the arithmetic operations execution in serial mode. The method assigns an Arithmetic Unit *(AU)* for the computation of each iteration (i).

The proposed optimization is based on the following observation: two successive iterations (i) and $(i+1)$ of algorithm 2 could be interleaved and executed in parallel. The iteration $(i+1)$ could start as soon as the last significant digit $S[0]_{(i)}$ of $S_{(i)}$ is obtained. In our method, a parameter w is defined which determines the degree of parallelization. w varies from 1 to $n+1$. If $w = n+1$, this leads to a full parallel execution of algorithm 2.

The computation complexity $CcpMMM(w,n)$ of algorithm 2 based on parallel execution according to w and n, is evaluated by the following expression:

$$CcpMMM(w,n) \simeq (n+2)\,(\lfloor n/w \rfloor + 1) \quad (5)$$

At the origin, the main objective of this method is to reduce the complexity $CcMMM$ defined in equation (4) by a factor inversely proportional to w. Indeed, from equation (5), we note that $CcMMM$ is divided by w.

In this work, our aim is not the optimization of the MMM computation throughput, but the achievement of the best trade-off between area and execution time. Therefore, we focus in our study for the implementations of the cases: $w = 1$ and $w = 2$.

IV. FPGA Implementation

In the following, we begin by the description of the internal circuit of the designed *AU*. Then, we present the FPGA implementation of the *MMMulr* multiplier based on our *AU* and on parallel execution of algorithm 2. Finally, we provide in detail the proposed approach for the implementation of the ME in the embedded system.

A. Arithmetic Unit Structure

The hardware architecture of the *AU* is shown in Fig1. This unit is dedicated to the execution of the basic arithmetic operations of algorithm 2. The *AU* consists of:

a. two $32-bits$ multipliers *Mul1* and *Mul2*,
b. four $32-bits$ carry propagate adders *Add1*, *Add2*, *Add3* and *Add4*,
c. four registers *R1*, *R2*, *R3* and *R4*,
d. four *D* flip-flops,
e. two multiplexers *Mux1* and *Mux2*.

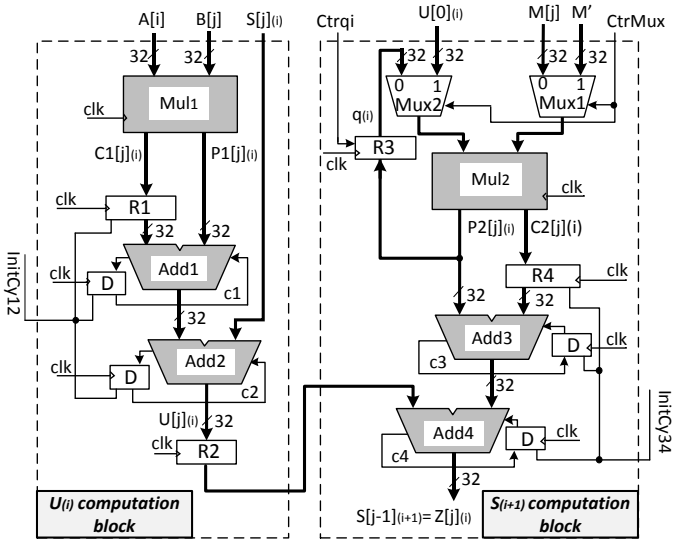


Fig 1. Hardware architecture of the arithmetic unit

At each computation cycle, one $32-bits$ digit of the intermediate result $S_{(i+1)}$ is provided at the *AU* output. The computation process is based on four control signals $CtrMux$, $Ctrq_i$, $InitCy12$ and $InitCy34$.

$CtrMux$ ensures the selection of the data at the inputs of *Mux1* and *Mux2*. $Ctrq_i$ allows for maintaining the $q_{(i)}$ value constant during the execution of the $(i)th$ iteration of algorithm 2. $InitCy12$ and $InitCy34$ are used for controlling the initialization of the generated carries.

The *AU* performs each iteration (i) of algorithm 2 in three steps. In the first step, the process begins by the execution of line 5 for computing the digit $q_{(i)}$. The obtained value is stored in the register *R3*. The second and the third steps consist in the execution of the equations defined from line 9 to line 12. They allow the computations of the digits $U[j]_{(i)}$ and $S[j-1]_{(i+1)}$, respectively. $U[j]_{(i)}$ is calculated using *Mul1*, *add1* and *add2*. $S[j-1]_{(i+1)}$ is computed by *Mul2*, *Add3* and *Add4*.

At each iteration *(j)*, the generated carries and the computed most significant digits $C1[j]_{(i)}$ and $C2[j]_{(i)}$ of the

multiplications $A[i]\times B[j]$ and $q_{(i)}\times M[j]$ are delayed by one clock cycle and added at the next iteration *(j+1)*.

The multiplier *Mul2* is shared between both multiplications:

- $U[0]_{(i)} \times M'$ of line 5 for computing $q_{(i)}$
- $q_{(i)}\times M[j]$ of line 11.

The selection of the operands at the inputs of this multiplier is ensured by the multiplexers *Mux1* and *Mux2*, according to the $CtrMux$ signal.

In order to increase the MMM computation throughput, our *AU* is designed, using two strategies:

- The pipeline processing is applied for getting the digits $S[j]_{(i+1)}$ of the intermediates results.
- Increasing the pipeline depth in order to reduce the clock cycle.

To obtain two successive digits $S[j-1]_{(i+1)}$ and $S[j]_{(i+1)}$ considering $A[i]$ and $q_{(i)}$ constants, the steps are presented in Fig 2.

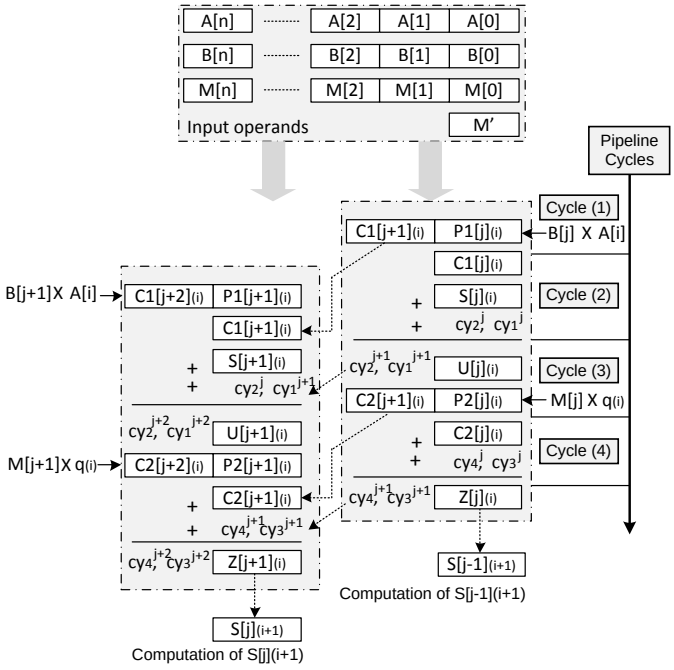


Fig. 2 Arithmetic unit pipeline cycles

Using the proposed scheme, the *AU* latency is defined by the required Clock cycle count ($CccAU$) to get a single digit $S[j]_{(i+1)}$. *CccAU* is about 4 clock cycles.

As it is motioned in section III, single iteration (i) of algorithm 2 is completely executed after $n+2$ cycles. Taking into account the *AU* latency, the intermediate result $S_{(i+1)}$ will be fully obtained after $n+6$ clock cycles.

B. Montgomery Modular Multiplier (MMMulr) Architecture

The *MMMulr* top level architecture based on two degrees of parallelization ($w=2$) is show in Fig 3. It consists in the implementation of two parallels *AU* (*AU1* and *AU2*).

Using the proposed approach, we consider that two successive iterations (i) and $(i+1)$ are interleaved and performed in parallel. The second iteration starts as soon as the least significant digit $S[0]_{(i+1)}$ is computed by the first iteration. Both iterations are delayed by the *AU* latency. In case of $w=1$, the architecture is implemented with only one *AU*. This means that all the iteration (i) of algorithm 2 are computed in sequential.

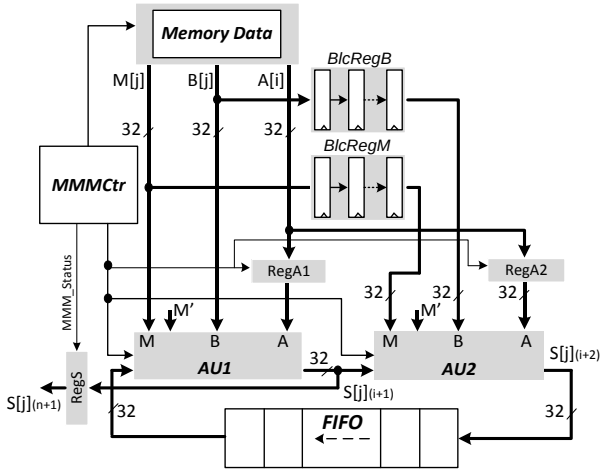


Fig 3. Hardware architecture of *MMMulr*

MMMulr is composed by the following components:

a. *Memory data:* contains the operands A, B and the modulus M.
b. *Two arithmetic units AU1 and AU2:* used for the parallel execution of two iterations (i) and $(i+1)$, to get the intermediates results $S_{(i+1)}$ and $S_{(i+2)}$, respectively.
c. *Two blocks 32-bits registers BlcRegB and BlcRegM*: since the last significant digit $S[0]_{(i+1)}$ of $S_{(i+1)}$ is obtained after the *AU* latency, *BlcRegB* and *BlcRegM* allow delaying the digits of the operands *B* and *M* with the required delay. In other words, they ensure the synchronization at the *AU2* inputs of the operands and the intermediate result $S_{(i+1)}$.
d. *Two 32-bits registers RegA1* and *RegA2*: used for keeping constant the digits $A[i]$ and $A[i+1]$ of operand A at the inputs of the units *AU1* and *AU2*, during the execution of the iterations (i) and $(i+1)$, respectively. It should be noted that the reading of $A[i]$ and of $A[i+1]$ are delayed between them with the respect latency of *AU1*.
e. *One memory FIFO:* ensures the transfer as queue of the intermediate result $S_{(i+2)}$ to the input of *AU1*. Indeed, for computing the next successive intermediates results $S_{(i+3)}$ and $S_{(i+4)}$ and completing the remainder of the execution process, the output of *AU2* is looped to the input of *AU1* through this memory.
f. *One 32-bits register RegS:* used to collect the $32-bits$ digits of the MMM result $S_{(n+1)}$.

These components are synchronized by a control circuit *(MMMCtr)*. It allows:

- the generation of the memory addresses (write/read addresses) and their control signals;
- the generation of the control signals of *AU1* and *AU2* units;
- the control of the registers (*RegA1* and *RegA2*) and of the blocks registers (*BlcRegB* and *BlcRegM*);
- the generation of *MMM_Status* signal which allows checking the *MMMulr* status.

The MMM Clock cycle count $CccMMMulr\,(w,n)$ for achieving single MMM by the proposed *MMMulr* multiplier is evaluated, considering two aspects:

1. Our *MMMulr* architecture is deducted from the parallel execution of algorithm 2. The computation complexity $CcpMMM(w,n)$ is given by equation (5).
2. The *AU* performance to execute a single iteration of MMM algorithm. The corresponding complexity in terms of clock cycle count is about $n+6$.

$CccMMMulr(w,n)$ is calculated by the following equation:

$$CccMMMulr(w,n) = (n+6) \times (\lfloor n/w \rfloor + 1) \quad (6)$$

C. Microblaze-Based PSoC Architecture

The hardware architecture of the proposed embedded PSoC is show in Fig 4. It is composed by the processor Microblaze and the dedicated accelerator ME co-processor. Other components are added; namely, memory BRAM, Local Memory Bus (LMB), Processor Local Bus (PLB), Universal Asynchronous Receiver Transmitter (UART) and Timer. These components are the basic peripherals. They are integrated in order to ensure the running of the system and to verify its functionality. The UART allows the communication between the processor and the RS232 port of the board. The Timer is used to compute the required clock cycles number for executing single modular exponentiation. Microblaze receives the instructions and the data through the buses ILMB and DLMB, respectively. All the peripherals communicate with Microblaze through the PLB bus.

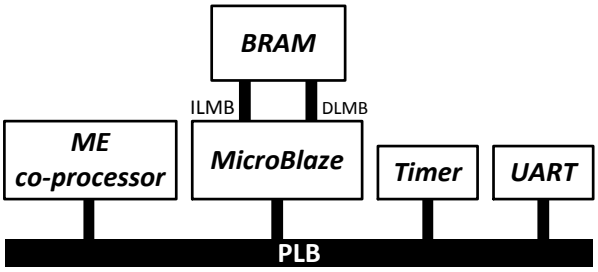


Fig 4. . Hardware architecture of the embedded system

The SW part of the PSoC is built based on the device drivers of each peripheral of the embedded system. It is implemented using C code.

The important component of our embedded system is the designed co-processor. In the following, let us consider its HW/SW co-design.

D. HW/SW co design of the ME co-processor

In order to improve the execution speed of the MPL algorithm, two parallels Montgomery modular multipliers are integrated within the ME-coprocessor. In addition, to reduce the data transfer between Microblaze and the ME co-processor, during the ME execution, the required data composed by the exponent E, the modulus M, X, both constants ($R^2 \bmod M$ and M') and data length are transmitted one time, at the beginning of the ME execution. The intermediate results $R0_{(i)}$ and $R1_{(i)}$ of MPL algorithm are stored in local memory, close to both multipliers. In software, the assigned tasks are limited to enabling/disabling the ME co-processor functionalities and to the input/output transfers.

The block diagram of the proposed ME co-processor is shown in Fig.5. Its HW/SW co-design requires the development of three parts.

- The first is the system communication interface. It allows the communication between Microbaze and the co-processor [14].
- The second is an integrated hardware *ModExp* core which ensures the parallel execution of the MMMs, based on MPL algorithm. It consists mainly of block memories, two parallel *MMMulr's* multipliers, control circuit and registers.
- The third is the SW device driver which is executed by the processor.

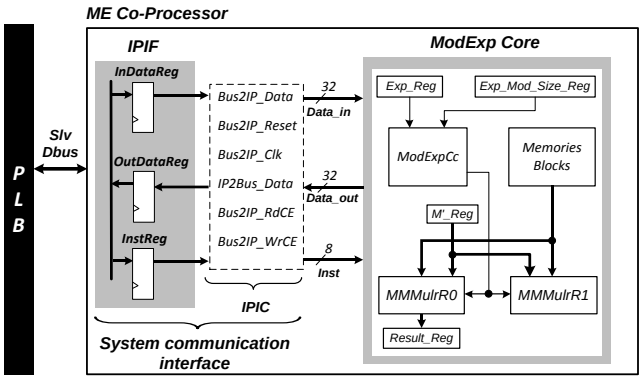


Fig.5 . Block diagram of ME Co-processor

V. Implementation Results and Discussion

The hardware architectures of the *AU* and the *MMMulr* were synthesized using ISE 3.2 (Xilinx Integrated Software Environment) tool. The designed hardware architectures were coded using VHDL language. Our *AU* was described in parameterable code, such that it is scalable and independent of operands length. The memory blocks and DSP48E cores were generated with the Core Generator tool. The HW/SW co-design of the ME co-processor and of our PSoC embedded system were realized using EDK (Embedded Design Kit) 13.2. The PSoC functionally was verified using Virtex-5 XC5VLX50T Genesys development board [15]. ModelSim SE 6.4 10.0C was used for the verification of the overall hardware architectures.

The execution performances of our design strategies are analyzed based on two aspects:

1. The parallelization degree defined by the w parameter. In order to achieve the optimum trade-off between the execution time and the area, our study is limited to one and two degrees of parallelization ($w=1$ and $w=2$). Recall that when $w=1$, the *MMMulr* multipler is designed with only one *AU*. If $w=2$, this mean that *MMMulr* is implemented with two *AU's*.
2. The security level size ($m-bits$,$t-bits$). m and t are the bits-width of the modulus and of the exponent, respectively. In our work, three security levels are considered, namely, $(512-bits, 512-bits)$, $(1024-bits, 1024-bits)$ and $(2048-bits, 2048-bits)$.

Comparisons of the proposed approaches are related to :

- The execution performance of the multiplier *MMMulr* for computing single MMM. The results are reported, considering only the pure hardware implementation of this operation.
- The execution time and the requirement of hardware resources of our embedded system for the execution of single ME.

A. Timing Performance

The timing performances of the proposed *MMMulr* and of the embedded ME co-processor, according to both parameters w and security level (m, t), are shown in Table I.

In this table, f_{max} represents the maximal frequency, computed such that $f_{max} = {}^{1}/_{t_{clk}}$. t_{clk} is the clock period closely linked to the critical path of the *AU*. It is reported by the timing reports of ISE tool. Indeed, in the *AU* architecture, t_{clk} is determined by the pipeline stage having the maximal delay (see Fig 1). This delay corresponds to the computation times of the products $A[i] \times B[j]$ or $q(i) \times M[j]$ which require one $32 - bits$ multiplier. The performances evaluation of the ME within the PSoC is carried out using a frequency $f = 100\ Mhz$.

TABLE I. MMMULR AND ME CO-PROCESSOR TIMING PERFORMNACE

Parameters			MMMulr timing performances				
Security level (m, t) (bits, bits)	n	w	f_{max} (Mhz)	CccMMMulr (w,n)	t_{MMM} (µs)	f (Mhz)	t_{ME} (ms)
(512,512)	16	1	107	374	3.48	100	2.08
		2	104	198	1.90	100	1.12
(1024,1024)	32	1	109	1254	11.43	100	12.94
		2	103	646	6.24	100	6.75
(2048,2048)	64	1	107	4550	42.23	100	93.42
		2	102	2310	22.62	100	47.91

$CccMMMulr(w, n)$ is the clock cycles count of the *MMMulr* for computing single MMM.

t_{MMM} denotes the execution time of the MMM. This delay is computed by the multiplication $CccMMMulr(w, n) \times t_{clk}$.

t_{ME} is the ME co-processor execution time. It is obtained by the multiplication of the necessary clock cycles given by the Timer with the clock period. t_{ME} includes the delays required for receiving all the inputs data from the local memory BRAM of Microblaze and for transmitting back the ME result.

Through the results, we note that the degree of parallelization and the security level have a great influence on the execution times of our ME coprocessor. The timing results show that the used of two parallels *AU's* within the *MMMulr* multiplier allows the optimizations of t_{MMM} and t_{ME}.

Indeed, considering a fixed security level, the MMM and the ME computations with two degree of parallelization ($w = 2$) induce an execution speed almost 2 times faster than the results obtained with one degree of parallelization. For example, if we consider the security level $(1024 - bits, 1024 - bits)$, the three delays obtained with one degree of parallelization ($w = 1$) are approximately divided by 2, when using $w = 2$.

B. Requirements of Hardware Resources

The occupied hardware resources by the implemented *MMMulr* and the proposed embedded system on the target FPGA circuit XC5VLX50TFFG1136, are shown in Table II.

The results are listed in terms of number of slices, of blocks RAM (36 Kbits and 18 Kbits) and of DSP48E cores.

The comparison between the implementations using one and two degrees of parallelization shows that the improvement of the execution times requires an additional cost. In fact, for a fixed security level, the implementation results shows that when using $w = 2$, the occupied slices increases. The DSP48E cores number is multiplied by 2.

The requirements of hardware resources obtained with the change of the security level while keeping the degree of parallelization constant is the most interested result. Indeed, the hardware resources numbers remain almost close, when the security level increases. The result confirms that the occupied area is not only independent of the security level, but also our approaches are efficient for the MMM and for the ME implementations in a PSoC platform.

Through the performances execution results, the implementation of ME using $w = 2$ represents the best profile in terms of execution time. In fact, compared to embedded system with $w = 1$, although the occupied resource number increases, the improvement of the execution time is more important. Thus we can consider that the use of the two degrees of parallelization is the best implementation which leads to an optimum trade-off between execution time and occupied area.

Table III compares our HW/SW co-design of the ME with the execution performances reached by some recent works.

The comparisons are based on the execution time, the requirement of hardware resources and the product (t_{ME}× Slice). In this table, the column "Embedded Processor" is added in order to show if the design integrates an embedded processor.

In [13], two implementation approaches for flexible HW/SW co-design of ME have been realized. This work was based on R2L and digit-serial $radix - 2^{32}$ algorithms for $1024 - bits$ ME and MMM executions. The soft processor core Microblaze is used for flexibility. The HW/SW partitioning consisted in the integration around the processor of two parallel MM multipliers. The control of the exponent was executed in SW. This work is better than our PSoC embedded system in terms of the requirements hardware resources. For a security level $(1024 - bits, 1024 - bits)$, the difference is about 1033 slices. However, our implementation approach is approximately 3.33 times faster.

L.R.Flores et al in [16] present HW/SW co-design of compact ME, based on Zynq 7000 platform and MPL digit-by-digit algorithm. The reported comparison shows that our design is better in terms of execution time. The ME computation is 2.33 times faster. The advantage of *Flores* work is linked to the occupied slices number which is about 459 slices. However, the presented implementation integrates a hard core Cortex-A9

Table II . HARDWARE RESOURCE REQUIREMENTS FOR THE MMMULR AND FOR THE EMBEDDED SYSTEM

Parameters			MMMulr hardware resources			Embedded system hardware resources			
Security level (m,t) (bits,bits)	n	w	Area (Slices)	Select RAM (18Kbits)	DSP48E (Cores)	Area (Slices)	Select RAM (18Kbits)	Select RAM (36Kbits)	DSP48E (Cores)
(512, 512)	16	1	240	4	8	2439	9	4	16
		2	623	4	16	2649	9	4	32
(1024, 1024)	32	1	243	4	8	2390	9	4	16
		2	647	4	16	2881	9	4	32
(2048, 2048)	64	1	243	4	8	2433	9	4	16
		2	636	4	16	2824	9	4	32

TABLE III . PERFORMANCE COMPARISON WITH PREVIOUS MODULAR EXPONENTIATION

	f (Mhz)	Design approach	Embedded processor	Security level (bits, bits)	time (ms)	Area (Slice Blocks RAM, DSP48E)			t_{ME}×Slice	Device
						Slices	Blocks RAM	DSP48E		
Our work	100	HW/SW	Yes	(512,512)	1.12	2649	9	32	2966	Virtex-5
				(1024,1024)	6.75	2881	9	32	19446	
[13]	62.5	HW/SW	Yes	(1024,1024)	22.5	1848	11	22	41580	Virtex-5
[16]	65	HW/SW	Yes	(1024,1024)	15.76	459	6	22	7233	Zynq-7000
[17]	111	HW/SW	No	(1024,1024)	17.12	27467	-	-	470235	Virtex-4
[18]	200	HW	No	(1024,1024)	6.79	5730	-	-	38906	Virtex-5

processor. In our embedded system design, the occupied slices include the requirement number for the Microblaze implementation (1038 slices).

Usadel et al present in [17] a HW/SW co-design of the ME, based on R2L and Chinese Remainder Theorem algorithms. In this work, 8051 microcontroller is used as off-chip controller. The ME is realized on FPGA circuit as pure HW implementation. In terms of execution time, our architecture is better by approximately 60.57 % and requires less of slices.

In [18] *Z. Wang et al* present a pure HW design of a dedicated ME co-processor. From the execution times comparison, our HW/SW co-design is faster even if the *Wang* work is carried out in HW only, without an embedded processor. On the other hand, in terms of occupied slices number, our PSoC requires 1.98 times less than the ME co-processor of this work.

VI. CONCLUSION

In this paper, we have presented implementations of a scalable MM multiplier and of flexible ME co-processor on PSoC platform. The processor Microblaze of Xilinx is used for managing and updating the functionalities of our embedded system. The adopted design methodology led us to design efficient HW architectures which take into account several constraints. Indeed, the ME co-processor is parameterized in SW, able to operate with different exponents and data sizes. The arithmetic operations of the MMM algorithm are performed within a scalable *AU*, in digit-serial way. In order to generalize and to support high security levels, the *AU* was implemented with fixed data path, smaller than the operands length. Our optimization approach was based on the combination of: (i) the high $radix - r$ ($r = 2^{32}$) FIOS MMM algorithm, (ii) the pipeline processing and (iii) the parallel execution of the ME. At the high abstraction level of the ME implementation, we have proposed the integration of two parallel MM multipliers, inside the ME co-processor.

In perspective, we project to evaluate the execution performances of the proposed ME co-processor on Zynq-7000 FPGA circuit, using high degrees of parallelization.

ACKNOWLEDGMENT

The authors would like to thank the Directorate General for Scientific Research and Technological Development of Algeria for its support.

REFERENCES

[1] W. Diffie and M.E. Hellman, "New Directions in Cryptography", *IEEE Transactions on Information Theory*, vol.IT22, No.6, pp.644-654, 1976.

[2] R.L. Rivest, A. Shamir, and L. Adleman, "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems", Communication. ACM, vol 21, No.2, pp.120-126, 1978.

[3] C. Paar and J. Pelzl, "*Understanding Cryptography*", pp. 277-280, (Springer-Verlag 2010).

[4] M.Anane, H.Bessalah , M.Issad, N.Anane and H.Salhi "Higher radix and redundancy factor for floating point SRT Division", *IEEE Transaction On Very Large Scale Integration Systems*, vol.16, No.16, pp. 122-128, June 2008.

[5] P.Montgomery, "Modular Multiplication Without Trial Division", *Mathematics of Computation*, vol.44, pp.519-521, 1985.

[6] M. Joye, and S.M.Yen, "The Montgomery Powering Ladder", In *Proc Fourth Int'l Workshop Cryptographic Hardware and Embedded Systems CHES' 2002, pp. 291–302.*

[7] "MicroBlaze Processor Reference Guide", UG081 (v13.2).

[8] S.B.Ors, L.Batina, B.Preneel and J.Vandewalle, "Hardware Implementation of a Montgomery Modular Multiplier in a Systolic Array", In *Proc. 17th International Parallel & Distributed Processing Symposium*, IEEE Computer Society, 2003.

[9] S.S. Erdem, T.Yanik, and A.Çelebi, "A General Digit-Serial Architecture for Montgomery Modular Multiplication", IEEE Transactions On Very Large Scale Integration Systems, Vol. 25, No. 5, pp.1658-1668, May 2017.

[10] A.Rezai and P.Keshavarzi, "High-Throughput Modular Multiplication and Exponentiation Algorithms Using Multibit-Scan–Multibit-Shift Technique", *IEEE Transactions on Very Large Scale Integration Systems*, Vol. 23, No. 9, pp.1710-1719, September 2015.

[11] C. McIvor, M. McLoone, J. McCanny, A. Daly and W. Marnane, "Fast Montgomery Modular Multiplication and RSA Cryptographic Processor Architectures", In *Proc. 37th Annual Asilomar Conference on Signals, Systems and Computers*, pp.379–384, 2003.

[12] C.K.Koc, T.Acar, S.Burton and J.Kaliski, "Analyzing and Comparing Montgomery Multiplication Algorithms", *IEEE Micro*, Vol.16, No.33, pp.26-33, 1996.

[13] M. Issad, B. Boudraa, M. Anane, and N. Anane. "Software/hardware co-design of modular exponentiation for efficient RSA cryptosystem". Journal of Circuits, Systems, and Computers, Vol.23, No 3, pp.1-28, 2014.

[14] "PLB IPIF", DS448 (v2.02a), 2005.

[15] Genesys Board, Reference Manual, Revision, 2012.

[16] L.R.Flores, M.M.Sandoval, R.Cumplido, C.F.Uribe and I.A.Badillo, "Compact FPGA Hardware Architecture for Public Key Encryption in Embedded Devices", *https://doi.org/10.1371/journal.pone.0190939*, pp.1-21, January 2018.

[17] L. Uhsadel, M. Ullrich, I.Verbauwhede and B. Preneel, "Interface Design for Mapping a Variety of RSA Exponentiation Algorithms on a HW/SW Co-design Platform". In *Proc. 23rd International Conference on Application-Specific Systems, Architectures and Processors*, pp.109 – 116, 2012. 17

[18] Z. Wang, Z. Jia, L. Ju and R. Chen "ASIP-Based Design and Implementation of RSA for Embedded Systems", In *Proc. 14th IEEE International Conference on High Performance Computing and Communications* pp.1375-1382, 2012.

A Presentation of a Linear Code over $\mathcal{A}_{q,3} = \mathbb{Z}_q\left[u_1, u_2, u_3\right] \diagup \left\langle u_i^2 = 1, u_i u_j = u_j u_i \right\rangle$

*Note: Sub-titles are not captured in Xplore and

1st Karima. Chatouh
Faculty of Mathematics and informatics.
Department of Mathematics, Mostefa Ben Boulaïd University, Batna 2.
Batna, Algeria
karima.chatouh@gmail.com

***Abstract*—In this work, we introduce some explicit construction of codes over $\mathcal{A}_{q,3} = \mathbb{Z}_q\left[u_1, u_2, u_3\right] \diagup \langle u_i^2 = 1, u_i u_j = u_j u_i \rangle$, where $u_i^2 = 1$ and $u_i u_j = u_j u_i$, for $1 \leq i \neq j \leq 3$. We are interested in the presentation of these codes and their Gray images.**

***Index Terms*—Codes over finite rings, Gray map, Linear codes, The Lee weight.**

I. Introduction

Nowadays, information are almost completely transited in a digital form over a large variety of medium with different quantities, debits and impressive services. All this paved the way to the appearance of so many disciplines for which research is still active, for instance, the theory of the correcting codes or the cryptography [1], [2] and [3].

The errors correcting codes used to enhance the reliability of information exchange over a noisy channel. They are used in most modern technologies of communication.

Coding Theory is a large field of research, it is identifies the study of codes over rings. It is necessary to give the properties of these codes.

First, we are going to present some algebraic structures of linear codes over finite rings, and give certain properties of these codes. We will define some families of linear codes over finite fields which are Gray images. We are basically interested in families of codes over fields as well as in those of codes over $\mathcal{A}_{q,3}$. We are also interested in some properties of these codes.

The set of these results were obtained because of being interested in the study of linear codes over $\mathcal{A}_{q,3}$.

We are starting, in section II, by giving a brief introduction about ring $\mathcal{A}_{q,3}$ and linear correcting codes over this ring.

Section III, would be about calculating the Gray map which is used in finding the Gray images of linear codes over $\mathcal{A}_{q,3}$.

Identify applicable funding agency here. If none, delete this.

Linear codes over $\mathcal{A}_{q,3}$ are presented in details in section IV.

II. Preliminaries

The commutative ring $\mathcal{A}_{q,3} = \mathbb{Z}_q + u_1\mathbb{Z}_q + u_2\mathbb{Z}_q + u_3\mathbb{Z}_q + u_1u_2\mathbb{Z}_q + u_1u_3\mathbb{Z}_q + u_2u_3\mathbb{Z}_q + u_1u_2u_3\mathbb{Z}_q$.

If $a \in \mathcal{A}_{q,3}$, then $a = a_0 + u_1a_1 + u_2a_2 + u_3a_3 + u_1u_2a_4 + u_1u_3a_5 + u_2u_3a_6 + u_1u_2u_3a_7$.

We first establish some terminology, by a linear code C over a ring $\mathcal{A}_{q,3}$.

A linear code C of length n over $\mathcal{A}_{q,3}$ is defined to be an $\mathcal{A}_{q,3}$-module of $\mathcal{A}_{q,3}^n$.

Let $x = (x_1, x_2, \ldots, x_n)$ and $y = (y_1, y_2, \ldots, y_n)$ be any two elements of $\mathcal{A}_{q,3}^n$, we define the inner product over $\mathcal{A}_{q,3}$ as

$$\langle x, y \rangle_{\mathcal{A}_{q,3}} = \sum_{i=1}^{i=n} x_i y_i,$$

The dual code $C^\perp$ of C is defined by

$$C^\perp = \{x \in \mathcal{A}_{q,3}^n | \langle x, y \rangle_{\mathcal{A}_{q,3}} = 0 \text{ for all } y \in C\}$$

If $C \subset C^\perp$, we say the code is self-orthogonal, and if $C = C^\perp$ then we say the code is self-dual.

III. The Gray Map and the Gray Images of linear codes over $\mathcal{A}_{q,3}$

We define the Gray map for to the Lee weight by:

$$\begin{array}{rccc} \Phi_{Lee} & : & \mathcal{A}_{q,3} & \to & \mathbb{Z}_q^8 \\ & & x & \mapsto & \Phi_{Lee}(x), \end{array} \tag{1}$$

with,

$\Phi_{Lee}(x = x_0 + u_1x_1 + u_2x_2 + u_3x_3 + u_1u_2x_4 + u_1u_3x_5 + u_2u_3x_6 + u_1u_2u_3x_7) = ((x_0 + x_1 + x_2 + x_3 + x_4 + x_5 + x_6 +$

$x_7), (x_0+x_1+x_2-x_3+x_4-x_5-x_6-x_7), (x_0+x_1-x_2-x_3-x_4-x_5+x_6+x_7), (x_0+x_1-x_2+x_3-x_4+x_5-x_6-x_7), (x_0-x_1+x_2+x_3-x_4-x_5+x_6-x_7), (x_0-x_1-x_2+x_3+x_4-x_5-x_6+x_7), (x_0-x_1+x_2-x_3-x_4+x_5-x_6+x_7), (x_0-x_1-x_2-x_3+x_4+x_5+x_6-x_7))$.

Can be extended this application to $\mathcal{A}_{q,3}^n$ we have,

$$\begin{array}{rccc} \Phi_{Lee} & : & \mathcal{A}_{q,3}^n & \to & \mathbb{Z}_q^{8n} \\ & & x=(x_0,x_1,x_2,x_3,x_4,x_5,x_6,x_7) & \mapsto & \Phi_{Lee}(x), \end{array}$$

where, $x_i = x_0^i + u_1x_1^i + u_2x_2^i + u_3x_3^i + u_1u_2x_4^i + u_1u_3x_5^i + u_2u_3x_6^i + u_1u_2u_3x_7^i$ for $i = 0, 2, 3, 4, 5, 6, 7$.

The Lee weight of $x \in \mathcal{A}_{q,3}$ as $w_{Lee}(x) = w_{Ham}(x)$, where w_{Ham} is the Hamming weight.

For any element $x, x \in \mathcal{A}_{q,3}$, the Lee distance is given by $d_{Lee}(x, y) = w_{Lee}(x - y)$.

From the definition of the Gray map is obvious we recognize the following results.

Theorem 3.1: The Gray map is an isometry from

$$(\mathcal{A}_{q,3}^n, \text{Lee distance}) \to (\mathbb{Z}_q^{8n}, \text{Hamming distance})$$

Proof.

By the definition of of the Gray map we notice that Φ_{Lee} is a linear application, on the other hand Φ_{Lee} is a distance-preserving map because,

$$\begin{array}{rcl} d_{Lee}(x,y) & = & w_{Lee}(x-y) \\ & = & w_{Ham}(\Phi_{Lee}(x-y)) \\ & = & w_{Ham}(\Phi_{Lee}(x)-\Phi_{Lee}(y)) \\ & = & d_{Ham}(\Phi_{Lee}(x),\Phi_{Lee}(y)). \end{array}$$

■

Theorem 3.2: If C is a linear code of length n over $\mathcal{A}_{q,3}$ with, minimum Lee distance d_{Lee}, then $\Phi_{Lee}(C)$ is a linear code of length $8n$ over $\mathbb{Z}_q$.

Theorem 3.3: If C is self orthogonal, then $\Phi_{Lee}(C)$ is self orthogonal.

Proof.

$\forall x, y \in C$ (C is self orthogonal code), if $x = x_0 + u_1x_1 + u_2x_2 + u_3x_3 + u_1u_2x_4 + u_1u_3x_5 + u_2u_3x_6 + u_1u_2u_3x_7$ and $y = y_0 + u_1y_1 + u_2y_2 + u_3y_3 + u_1u_2y_4 + u_1u_3y_5 + u_2u_3y_6 + u_1u_2u_3y_7$,

then,

$x \cdot y = x_0y_0 + x_1y_1 + x_2y_2 + x_3y_3 + x_4y_4 + x_5y_5 + x_6y_6 + x_7y_7 + u_1((x_0y_1 + x_1y_0) + (x_2y_4 + x_4y_2) + (x_3y_5 + x_5y_3) + (x_6y_7 + x_7y_6)) + u_2((x_0y_2 + x_2y_0) + (x_1y_4 + x_4y_1) + (x_3y_6 + x_6y_3) + (x_5y_7 + x_7y_5)) + u_3((x_0y_3 + x_3y_0) + (x_1y_5 + x_5y_1) + (x_2y_6 + x_6y_2) + (x_4y_7 + x_7y_4)) + u_1u_2((x_0y_4 + x_4y_0) + (x_1y_2 + x_2y_1) + (x_3y_7 + x_7y_3) + (x_5y_6 + x_6y_5)) + u_1u_3((x_0y_5 + x_5y_0) + (x_2y_7 + x_7y_2) + (x_1y_3 + x_3y_1) + (x_4y_6 + x_6y_4)) + u_2u_3((x_0y_6 + x_6y_0) + (x_1y_7 + x_7y_1) + (x_2y_3 + x_3y_2) + (x_4y_5 + x_5y_4)) + u_1u_2u_3((x_0y_7 + x_7y_0) + (x_1y_6 + x_6y_1) + (x_2y_5 + x_5y_2) + (x_3y_4 + x_4y_3)) = 0,$

we conclude that,

$x_0y_0 + x_1y_1 + x_2y_2 + x_3y_3 + x_4y_4 + x_5y_5 + x_6y_6 + x_7y_7 = 0,$

$(x_0y_1 + x_1y_0) + (x_2y_4 + x_4y_2) + (x_3y_5 + x_5y_3) + (x_6y_7 + x_7y_6) = 0,$

$(x_0y_2 + x_2y_0) + (x_1y_4 + x_4y_1) + (x_3y_6 + x_6y_3) + (x_5y_7 + x_7y_5) = 0,$

$(x_0y_3 + x_3y_0) + (x_1y_5 + x_5y_1) + (x_2y_6 + x_6y_2) + (x_4y_7 + x_7y_4) = 0,$

$(x_0y_4 + x_4y_0) + (x_1y_2 + x_2y_1) + (x_3y_7 + x_7y_3) + (x_5y_6 + x_6y_5) = 0,$

$(x_0y_5 + x_5y_0) + (x_2y_7 + x_7y_2) + (x_1y_3 + x_3y_1) + (x_4y_6 + x_6y_4) = 0,$

$(x_0y_6 + x_6y_0) + (x_1y_7 + x_7y_1) + (x_2y_3 + x_3y_2) + (x_4y_5 + x_5y_40,$

$(x_0y_7 + x_7y_0) + (x_1y_6 + x_6y_1) + (x_2y_5 + x_5y_2) + (x_3y_4 + x_4y_3) = 0.$

On the other hand,

$\Phi_{Lee}(x) \cdot \Phi_{Lee}(y) = ((x_0+x_1+x_2+x_3+x_4+x_5+x_6+x_7), (x_0+x_1+x_2-x_3+x_4-x_5-x_6-x_7), (x_0+x_1-x_2-x_3-x_4-x_5+x_6+x_7), (x_0+x_1-x_2+x_3-x_4+x_5-x_6-x_7), (x_0-x_1+x_2+x_3-x_4-x_5+x_6-x_7), (x_0-x_1-x_2+x_3+x_4-x_5-x_6+x_7), (x_0-x_1+x_2-x_3-x_4+x_5-x_6+x_7), (x_0-x_1-x_2-x_3+x_4+x_5+x_6-x_7))((y_0+y_1+y_2+y_3+y_4+y_5+y_6+y_7), (y_0+y_1+y_2-y_3+y_4-y_5-y_6-y_7), (y_0+y_1-y_2-y_3-y_4-y_5+y_6+y_7), (y_0+y_1-y_2+y_3-y_4+y_5-y_6-y_7), (y_0-y_1+y_2+y_3-y_4-y_5+y_6-y_7), (y_0-y_1-y_2+y_3+y_4-y_5-y_6+y_7), (y_0-y_1+y_2-y_3-y_4+y_5-y_6+y_7), (y_0-y_1-y_2-y_3+y_4+y_5+y_6-y_7))$.

By the equations obtained previously we have,

$\Phi_{Lee}(x)\Phi_{Lee}(y) = 0$, it means that the code C is self orthogonal.

■

IV. A Linear Code over $\mathcal{A}_{q,3}$

The same methodology obtained in [4] and [5], we have.

If a be an element of $\mathcal{A}_{q,3}$, let,

$$\xi_0 = \frac{1}{8}(1+u_1+u_2+u_3+u_1u_2+u_1u_3+u_2u_3+u_1u_2u_3)$$

$$\xi_1 = \frac{1}{8}(1+u_1+u_2-u_3+u_1u_2-u_1u_3-u_2u_3-u_1u_2u_3)$$

$$\xi_2 = \frac{1}{8}(1+u_1-u_2-u_3-u_1u_2-u_1u_3+u_2u_3+u_1u_2u_3)$$

$$\xi_3 = \frac{1}{8}(1+u_1-u_2+u_3-u_1u_2+u_1u_3-u_2u_3-u_1u_2u_3)$$

$$\xi_4 = \frac{1}{8}(1-u_1+u_2+u_3-u_1u_2-u_1u_3+u_2u_3-u_1u_2u_3)$$

$$\xi_5 = \frac{1}{8}(1-u_1-u_2+u_3+u_1u_2-u_1u_3-u_2u_3+u_1u_2u_3)$$

$$\xi_6 = \frac{1}{8}(1-u_1+u_2-u_3-u_1u_2+u_1u_3-u_2u_3+u_1u_2u_3)$$

$\xi_7 = \frac{1}{8}(1 - u_1 - u_2 - u_3 + u_1u_2 + u_1u_3 + u_2u_3 - u_1u_2u_3)$

It is easy to show that $\xi_i^2 = \xi_i$, $\xi_i\xi_j = 0$, where $i \neq j \in \{0,1,2,3,4,5,6,7\}$ and $\sum_{i=1}^{8} \xi_i = 1$.

We can write a of the form,

$a = a_0 + u_1a_1 + u_2a_2 + u_3a_3 + u_1u_2a_4 + u_1u_3a_5 + u_2u_3a_6 + u_1u_2u_3a_7$,

and also of the form,

$$\begin{aligned} x = {} & \xi_0(x_0 + x_1 + x_2 + x_3 + x_4 + x_5 + x_6 + x_7) \\ & + \xi_1(x_0 + x_1 + x_2 - x_3 + x_4 - x_5 - x_6 - x_7) \\ & + \xi_2(x_0 + x_1 - x_2 - x_3 - x_4 - x_5 + x_6 + x_7) \\ & + \xi_3(x_0 + x_1 - x_2 + x_3 - x_4 + x_5 - x_6 - x_7) \\ & + \xi_4(x_0 - x_1 + x_2 + x_3 - x_4 - x_5 + x_6 - x_7) \\ & + \xi_5(x_0 - x_1 - x_2 + x_3 + x_4 - x_5 - x_6 + x_7) \\ & + \xi_6(x_0 - x_1 + x_2 - x_3 - x_4 + x_5 - x_6 + x_7) \\ & + \xi_7(x_0 - x_1 - x_2 - x_3 + x_4 + x_5 + x_6 - x_7). \end{aligned} \tag{2}$$

Let C be a linear code of length n over the ring $\mathcal{A}_{q,3}$ and let $C_0, C_1, C_2, C_3, C_4, C_5, C_6, C_7$ be a linear codes of length n over $\mathbb{Z}_q$. Where,

$C_0 = \{a_0 + a_1 + a_2 + a_3 + a_4 + a_5 + a_6 + a_7, \exists a_0, a_1, a_2, a_3, a_4, a_5, a_6, a_7 \in \mathbb{Z}_q, \text{ such as } a \in C\}$,

$C_1 = \{a_0 + a_1 + a_2 - a_3 + a_4 - a_5 - a_6 - a_7, \exists a_0, a_1, a_2, a_3, a_4, a_5, a_6, a_7 \in \mathbb{Z}_q, \text{ such as } a \in C\}$,

$C_2 = \{a_0 + a_1 - a_2 - a_3 - a_4 - a_5 + a_6 + a_7, \exists a_0, a_1, a_2, a_3, a_4, a_5, a_6, a_7 \in \mathbb{Z}_q, \text{ such as } a \in C\}$,

$C_3 = \{a_0 + a_1 - a_2 + a_3 - a_4 + a_5 - a_6 - a_7, \exists a_0, a_1, a_2, a_3, a_4, a_5, a_6, a_7 \in \mathbb{Z}_q, \text{ such as } a \in C\}$,

$C_4 = \{a_0 - a_1 + a_2 + a_3 - a_4 - a_5 + a_6 - a_7, \exists a_0, a_1, a_2, a_3, a_4, a_5, a_6, a_7 \in \mathbb{Z}_q, \text{ such as } a \in C\}$,

$C_5 = \{a_0 - a_1 - a_2 + a_3 + a_4 - a_5 - a_6 + a_7, \exists a_0, a_1, a_2, a_3, a_4, a_5, a_6, a_7 \in \mathbb{Z}_q, \text{ such as } a \in C\}$,

$C_6 = \{a_0 - a_1 + a_2 - a_3 - a_4 + a_5 - a_6 + a_7, \exists a_0, a_1, a_2, a_3, a_4, a_5, a_6, a_7 \in \mathbb{Z}_q, \text{ such as } a \in C\}$,

$C_7 = \{a_0 - a_1 - a_2 - a_3 + a_4 + a_5 + a_6 - a_7, \exists a_0, a_1, a_2, a_3, a_4, a_5, a_6, a_7 \in \mathbb{Z}_q, \text{ such as } a \in C\}$.

Then, the linear code C of length n over $\mathcal{A}_{q,3}$ can be uniquely expressed as,

$$C = \xi_0C_0 \oplus \xi_1C_1 \oplus \xi_2C_2 \oplus \xi_3C_3 \oplus \xi_4C_4 \oplus \xi_5C_5 \oplus \xi_6C_6 \oplus \xi_7C_7. \tag{3}$$

This writing of this code specifies several results, including the following.

Theorem 4.1: Let C be a linear code of length n over $\mathcal{A}_{q,3}$. Then $\Phi_{Lee}(C) = C_0 \otimes C_1 \otimes C_2 \otimes C_3 \otimes C_4 \otimes C_5 \otimes C_6 \otimes C_7$ and $|C| = |C_0||C_1||C_2||C_3||C_4||C_5||C_6||C_7|$.

Proof. $\forall (y^{(0)}, y^{(1)}, y^{(2)}, y^{(3)}, y^{(4)}, y^{(5)}, y^{(6)}, y^{(7)}) \in \Phi_{Lee}(C)$ where, $y^{(0)} = y_0^{(0)}, \ldots, y_{n-1}^{(0)}$, $y^{(1)} = y_0^{(1)}, \ldots, y_{n-1}^{(1)}$, $y^{(2)} = y_0^{(2)}, \ldots, y_{n-1}^{(2)}$, $y^{(3)} = y_0^{(3)}, \ldots, y_{n-1}^{(3)}$, $y^{(4)} = y_0^{(4)}, \ldots, y_{n-1}^{(4)}$, $y^{(5)} = y_0^{(5)}, \ldots, y_{n-1}^{(5)}$, $y^{(6)} = y_0^{(6)}, \ldots, y_{n-1}^{(6)}$ and $y^{(7)} = y_0^{(7)}, \ldots, y_{n-1}^{(7)}$.

By the Theorem 3.1, Φ_{Lee} is a bijective application then, $\exists (x^0, x^1, \ldots, x^{n-1})! \in C$ such as,

$\Phi_{Lee}((x^0, x^1, \ldots, x^{n-1})) = (y^{(0)}, y^{(1)}, y^{(2)}, y^{(3)}, y^{(4)}, y^{(5)}, y^{(6)}, y^{(7)})$. But,

$x^0 = \xi_0(x_0^0 + x_1^0 + x_2^0 + x_3^0 + x_4^0 + x_5^0 + x_6^0 + x_7^0) + \xi_1(x_0^0 + x_1^0 + x_2^0 - x_3^0 + x_4^0 - x_5^0 - x_6^0 - x_7^0) + \xi_2(x_0^0 + x_1^0 - x_2^0 - x_3^0 - x_4^0 - x_5^0 + x_6^0 + x_7^0) + \xi_3(x_0^0 + x_1^0 - x_2^0 + x_3^0 - x_4^0 + x_5^0 - x_6^0 - x_7^0) + \xi_4(x_0^0 - x_1^0 + x_2^0 + x_3^0 - x_4^0 - x_5^0 + x_6^0 - x_7^0) + \xi_5(x_0^0 - x_1^0 - x_2^0 + x_3^0 + x_4^0 - x_5^0 - x_6^0 + x_7^0) + \xi_6(x_0^0 - x_1^0 + x_2^0 - x_3^0 - x_4^0 + x_5^0 - x_6^0 + x_7^0) + \xi_7(x_0^0 - x_1^0 - x_2^0 - x_3^0 + x_4^0 + x_5^0 + x_6^0 - x_7^0)$,

$x^1 = \xi_0(x_0^1 + x_1^1 + x_2^1 + x_3^1 + x_4^1 + x_5^1 + x_6^1 + x_7^1) + \xi_1(x_0^1 + x_1^1 + x_2^1 - x_3^1 + x_4^1 - x_5^1 - x_6^1 - x_7^1) + \xi_2(x_0^1 + x_1^1 - x_2^1 - x_3^1 - x_4^1 - x_5^1 + x_6^1 + x_7^1) + \xi_3(x_0^1 + x_1^1 - x_2^1 + x_3^1 - x_4^1 + x_5^1 - x_6^1 - x_7^1) + \xi_4(x_0^1 - x_1^1 + x_2^1 + x_3^1 - x_4^1 - x_5^1 + x_6^1 - x_7^1) + \xi_5(x_0^1 - x_1^1 - x_2^1 + x_3^1 + x_4^1 - x_5^1 - x_6^1 + x_7^1) + \xi_6(x_0^1 - x_1^1 + x_2^1 - x_3^1 - x_4^1 + x_5^1 - x_6^1 + x_7^1) + \xi_7(x_0^1 - x_1^1 - x_2^1 - x_3^1 + x_4^1 + x_5^1 + x_6^1 - x_7^1)$,

$\vdots$

$x^{n-1} = \xi_0(x_0^{n-1} + x_1^{n-1} + x_2^{n-1} + x_3^{n-1} + x_4^{n-1} + x_5^{n-1} + x_6^{n-1} + x_7^{n-1}) + \xi_1(x_0^{n-1} + x_1^{n-1} + x_2^{n-1} - x_3^{n-1} + x_4^{n-1} - x_5^{n-1} - x_6^{n-1} - x_7^{n-1}) + \xi_2(x_0^{n-1} + x_1^{n-1} - x_2^{n-1} - x_3^{n-1} - x_4^{n-1} - x_5^{n-1} + x_6^{n-1} + x_7^{n-1}) + \xi_3(x_0^{n-1} + x_1^{n-1} - x_2^{n-1} + x_3^{n-1} - x_4^{n-1} + x_5^{n-1} - x_6^{n-1} - x_7^{n-1}) + \xi_4(x_0^{n-1} - x_1^{n-1} + x_2^{n-1} + x_3^{n-1} - x_4^{n-1} - x_5^{n-1} + x_6^{n-1} - x_7^{n-1}) + \xi_5(x_0^{n-1} - x_1^{n-1} - x_2^{n-1} + x_3^{n-1} + x_4^{n-1} - x_5^{n-1} - x_6^{n-1} + x_7^{n-1}) + \xi_6(x_0^{n-1} - x_1^{n-1} + x_2^{n-1} - x_3^{n-1} - x_4^{n-1} + x_5^{n-1} - x_6^{n-1} + x_7^{n-1}) + \xi_7(x_0^{n-1} - x_1^{n-1} - x_2^{n-1} - x_3^{n-1} + x_4^{n-1} + x_5^{n-1} + x_6^{n-1} - x_7^{n-1})$.

We have,

$\Phi_{Lee}(\xi_0(x_0^0 + x_1^0 + x_2^0 + x_3^0 + x_4^0 + x_5^0 + x_6^0 + x_7^0) + \xi_1(x_0^0 + x_1^0 + x_2^0 - x_3^0 + x_4^0 - x_5^0 - x_6^0 - x_7^0) + \xi_2(x_0^0 + x_1^0 - x_2^0 - x_3^0 - x_4^0 - x_5^0 + x_6^0 + x_7^0) + \xi_3(x_0^0 + x_1^0 - x_2^0 + x_3^0 - x_4^0 + x_5^0 - x_6^0 - x_7^0) + \xi_4(x_0^0 - x_1^0 + x_2^0 + x_3^0 - x_4^0 - x_5^0 + x_6^0 - x_7^0) + \xi_5(x_0^0 - x_1^0 - x_2^0 + x_3^0 + x_4^0 - x_5^0 - x_6^0 + x_7^0) + \xi_6(x_0^0 - x_1^0 + x_2^0 - x_3^0 - x_4^0 + x_5^0 - x_6^0 + x_7^0) + \xi_7(x_0^0 - x_1^0 - x_2^0 - x_3^0 + x_4^0 + x_5^0 + x_6^0 - x_7^0), \xi_0(x_0^1 + x_1^1 + x_2^1 + x_3^1 + x_4^1 + x_5^1 + x_6^1 + x_7^1) + \xi_1(x_0^1 + x_1^1 + x_2^1 - x_3^1 + x_4^1 - x_5^1 - x_6^1 - x_7^1) + \xi_2(x_0^1 + x_1^1 - x_2^1 - x_3^1 - x_4^1 - x_5^1 + x_6^1 + x_7^1) + \xi_3(x_0^1 + x_1^1 - x_2^1 + x_3^1 - x_4^1 + x_5^1 - x_6^1 - x_7^1) + \xi_4(x_0^1 - x_1^1 + x_2^1 + x_3^1 - x_4^1 - x_5^1 + x_6^1 - x_7^1) + \xi_5(x_0^1 - x_1^1 - x_2^1 + x_3^1 + x_4^1 - x_5^1 - x_6^1 + x_7^1) + \xi_6(x_0^1 - x_1^1 + x_2^1 - x_3^1 - x_4^1 + x_5^1 - x_6^1 + x_7^1) + \xi_7(x_0^1 - x_1^1 - x_2^1 - x_3^1 + x_4^1 + x_5^1 + x_6^1 - x_7^1), \ldots, \xi_0(x_0^{n-1} + x_1^{n-1} + x_2^{n-1} + x_3^{n-1} + x_4^{n-1} + x_5^{n-1} + x_6^{n-1} + x_7^{n-1}) + \xi_1(x_0^{n-1} + x_1^{n-1} + x_2^{n-1} - x_3^{n-1} + x_4^{n-1} - x_5^{n-1} - x_6^{n-1} - x_7^{n-1}) + \xi_2(x_0^{n-1} + x_1^{n-1} - x_2^{n-1} - x_3^{n-1} - x_4^{n-1} - x_5^{n-1} + x_6^{n-1} + x_7^{n-1}) + \xi_3(x_0^{n-1} + x_1^{n-1} - x_2^{n-1} + x_3^{n-1} - x_4^{n-1} + x_5^{n-1} - x_6^{n-1} - x_7^{n-1}) + \xi_4(x_0^{n-1} - x_1^{n-1} + x_2^{n-1} + x_3^{n-1} - x_4^{n-1} - x_5^{n-1} + x_6^{n-1} - x_7^{n-1}) + \xi_5(x_0^{n-1} - x_1^{n-1} - x_2^{n-1} + x_3^{n-1} + x_4^{n-1} - x_5^{n-1} - x_6^{n-1} + x_7^{n-1}) + \xi_6(x_0^{n-1} - x_1^{n-1} + x_2^{n-1} - x_3^{n-1} - x_4^{n-1} + x_5^{n-1} - x_6^{n-1} + x_7^{n-1}) + \xi_7(x_0^{n-1} - x_1^{n-1} - x_2^{n-1} - x_3^{n-1} + x_4^{n-1} + x_5^{n-1} + x_6^{n-1} - x_7^{n-1})) = \xi_0\Phi_{Lee}((x_0^1 +$

$x_1^1+x_2^1+x_3^1+x_4^1+x_5^1+x_6^1+x_7^1), (x_0^1+x_1^1+x_2^1+x_3^1+x_4^1+x_5^1+x_6^1+x_7^1), \ldots, (x_0^{n-1}+x_1^{n-1}+x_2^{n-1}+x_3^{n-1}+x_4^{n-1}+x_5^{n-1}+x_6^{n-1}+x_7^{n-1})) + \xi_1\Phi_{Lee}((x_0^0+x_1^0+x_2^0-x_3^0+x_4^0-x_5^0-x_6^0-x_7^0), (x_0^1+x_1^1+x_2^1-x_3^1+x_4^1-x_5^1-x_6^1-x_7^1), \ldots, (x_0^{n-1}+x_1^{n-1}+x_2^{n-1}-x_3^{n-1}+x_4^{n-1}-x_5^{n-1}-x_6^{n-1}-x_7^{n-1})) + \xi_2\Phi_{Lee}((x_0^0+x_1^0-x_2^0-x_3^0-x_4^0-x_5^0+x_6^0+x_7^0), (x_0^1+x_1^1-x_2^1-x_3^1-x_4^1-x_5^1+x_6^1+x_7^1), \ldots, (x_0^{n-1}+x_1^{n-1}-x_2^{n-1}-x_3^{n-1}-x_4^{n-1}-x_5^{n-1}+x_6^{n-1}+x_7^{n-1})) + \xi_3\Phi_{Lee}((x_0^0+x_1^0-x_2^0+x_3^0-x_4^0+x_5^0-x_6^0-x_7^0), (x_0^1+x_1^1-x_2^1+x_3^1-x_4^1+x_5^1-x_6^1-x_7^1), \ldots, (x_0^{n-1}+x_1^{n-1}-x_2^{n-1}+x_3^{n-1}-x_4^{n-1}+x_5^{n-1}-x_6^{n-1}-x_7^{n-1})) + \xi_4\Phi_{Lee}((x_0^0-x_1^0+x_2^0+x_3^0-x_4^0-x_5^0+x_6^0-x_7^0), (x_0^1-x_1^1+x_2^1+x_3^1-x_4^1-x_5^1+x_6^1-x_7^1), \ldots, (x_0^{n-1}-x_1^{n-1}+x_2^{n-1}+x_3^{n-1}-x_4^{n-1}-x_5^{n-1}+x_6^{n-1}-x_7^{n-1})) + \xi_5\Phi_{Lee}((x_0^0-x_1^0-x_2^0+x_3^0+x_4^0-x_5^0-x_6^0+x_7^0), (x_0^1-x_1^1-x_2^1+x_3^1+x_4^1-x_5^1-x_6^1+x_7^1), \ldots, (x_0^{n-1}-x_1^{n-1}-x_2^{n-1}+x_3^{n-1}+x_4^{n-1}-x_5^{n-1}-x_6^{n-1}+x_7^{n-1})) + \xi_6\Phi_{Lee}((x_0^0-x_1^0+x_2^0-x_3^0-x_4^0+x_5^0-x_6^0+x_7^0), (x_0^1-x_1^1+x_2^1-x_3^1-x_4^1+x_5^1-x_6^1+x_7^1), \ldots, (x_0^{n-1}-x_1^{n-1}+x_2^{n-1}-x_3^{n-1}-x_4^{n-1}+x_5^{n-1}-x_6^{n-1}+x_7^{n-1})) + \xi_7\Phi_{Lee}((x_0^0-x_1^0-x_2^0-x_3^0+x_4^0+x_5^0+x_6^0-x_7^0), (x_0^1-x_1^1-x_2^1-x_3^1+x_4^1+x_5^1+x_6^1-x_7^1), \ldots, (x_0^{n-1}-x_1^{n-1}-x_2^{n-1}-x_3^{n-1}+x_4^{n-1}+x_5^{n-1}+x_6^{n-1}-x_7^{n-1})).$

So that,

$\Phi_{Lee}((x_0^1+x_1^1+x_2^1+x_3^1+x_4^1+x_5^1+x_6^1+x_7^1), (x_0^1+x_1^1+x_2^1+x_3^1+x_4^1+x_5^1+x_6^1+x_7^1), \ldots, (x_0^{n-1}+x_1^{n-1}+x_2^{n-1}+x_3^{n-1}+x_4^{n-1}+x_5^{n-1}+x_6^{n-1}+x_7^{n-1})) = y^{(0)} \in C_0,$

$\Phi_{Lee}((x_0^0+x_1^0+x_2^0-x_3^0+x_4^0-x_5^0-x_6^0-x_7^0), (x_0^1+x_1^1+x_2^1-x_3^1+x_4^1-x_5^1-x_6^1-x_7^1), \ldots, (x_0^{n-1}+x_1^{n-1}+x_2^{n-1}-x_3^{n-1}+x_4^{n-1}-x_5^{n-1}-x_6^{n-1}-x_7^{n-1})) = y^{(1)} \in C_1,$

$\Phi_{Lee}((x_0^0+x_1^0-x_2^0-x_3^0-x_4^0-x_5^0+x_6^0+x_7^0), (x_0^1+x_1^1-x_2^1-x_3^1-x_4^1-x_5^1+x_6^1+x_7^1), \ldots, (x_0^{n-1}+x_1^{n-1}-x_2^{n-1}-x_3^{n-1}-x_4^{n-1}-x_5^{n-1}+x_6^{n-1}+x_7^{n-1})) = y^{(2)} \in C_2,$

$\Phi_{Lee}((x_0^0+x_1^0-x_2^0+x_3^0-x_4^0+x_5^0-x_6^0-x_7^0), (x_0^1+x_1^1-x_2^1+x_3^1-x_4^1+x_5^1-x_6^1-x_7^1), \ldots, (x_0^{n-1}+x_1^{n-1}-x_2^{n-1}+x_3^{n-1}-x_4^{n-1}+x_5^{n-1}-x_6^{n-1}-x_7^{n-1})) = y^{(3)} \in C_3,$

$\Phi_{Lee}((x_0^0-x_1^0+x_2^0+x_3^0-x_4^0-x_5^0+x_6^0-x_7^0), (x_0^1-x_1^1+x_2^1+x_3^1-x_4^1-x_5^1+x_6^1-x_7^1), \ldots, (x_0^{n-1}-x_1^{n-1}+x_2^{n-1}+x_3^{n-1}-x_4^{n-1}-x_5^{n-1}+x_6^{n-1}-x_7^{n-1})) = y^{(4)} \in C_4,$

$\Phi_{Lee}((x_0^0-x_1^0-x_2^0+x_3^0+x_4^0-x_5^0-x_6^0+x_7^0), (x_0^1-x_1^1-x_2^1+x_3^1+x_4^1-x_5^1-x_6^1+x_7^1), \ldots, (x_0^{n-1}-x_1^{n-1}-x_2^{n-1}+x_3^{n-1}+x_4^{n-1}-x_5^{n-1}-x_6^{n-1}+x_7^{n-1})) = y^{(5)} \in C_5,$

$\Phi_{Lee}((x_0^0-x_1^0+x_2^0-x_3^0-x_4^0+x_5^0-x_6^0+x_7^0), (x_0^1-x_1^1+x_2^1-x_3^1-x_4^1+x_5^1-x_6^1+x_7^1), \ldots, (x_0^{n-1}-x_1^{n-1}+x_2^{n-1}-x_3^{n-1}-x_4^{n-1}+x_5^{n-1}-x_6^{n-1}+x_7^{n-1})) = y^{(6)} \in C_6,$

and,

$\Phi_{Lee}((x_0^0-x_1^0-x_2^0-x_3^0+x_4^0+x_5^0+x_6^0-x_7^0), (x_0^1-x_1^1-x_2^1-x_3^1+x_4^1+x_5^1+x_6^1-x_7^1), \ldots, (x_0^{n-1}-x_1^{n-1}-x_2^{n-1}-x_3^{n-1}+x_4^{n-1}+x_5^{n-1}+x_6^{n-1}-x_7^{n-1})) = y^{(7)} \in C_7.$

Then,

$(y^{(0)}, y^{(1)}, y^{(2)}, y^{(3)}, y^{(4)}, y^{(5)}, y^{(6)}, y^{(7)}) \in C_0 \otimes C_1 \otimes C_2 \otimes C_3 \otimes C_4 \otimes C_5 \otimes C_6 \otimes C_7.$

■

Theorem 4.2: If $G_0, G_1, G_2, G_3, G_4, G_5, G_6, G_7$ are generator matrices of $C_0, C_1, C_2, C_3, C_4, C_5, C_6, C_7$ respectively, then the generator matrix of C is

$$G = \begin{bmatrix} \xi_0 G_0 \\ \xi_1 G_1 \\ \xi_2 G_2 \\ \xi_3 G_3 \\ \xi_4 G_4 \\ \xi_5 G_5 \\ \xi_6 G_6 \\ \xi_7 G_7 \end{bmatrix}, \tag{4}$$

and,

$$\Phi_{Lee}(G) = \begin{bmatrix} \Phi(\xi_0 G_0) \\ \Phi(\xi_1 G_1) \\ \Phi(\xi_2 G_2) \\ \Phi(\xi_3 G_3) \\ \Phi(\xi_4 G_4) \\ \Phi(\xi_5 G_5) \\ \Phi(\xi_6 G_6) \\ \Phi(\xi_7 G_7) \end{bmatrix}$$

$$\Phi_{Lee}(G) = \begin{bmatrix} G_0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & G_1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & G_2 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & G_3 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & G_4 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & G_5 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & G_6 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & G_7 \end{bmatrix}$$

Proof. The proof is is a direct conclusion of Theorem 4.1. ■

Theorem 4.3: Let C be a linear code of length n over $\mathcal{A}_{(q,3)}$, then $\Phi(C^{\perp}) = [\Phi(C)]^{\perp}$. Further, C is a self-dual code if and only if $\Phi(C)$ is a self-dual code.

Proof. For $x = x_0 + u_1x_1 + u_2x_2 + u_3x_3 + u_1u_2x_4 + u_1u_3x_5 + u_2u_3x_6 + u_1u_2u_3x_7 \in C$ and $y = y_0 + u_1y_1 + u_2y_2 + u_3y_3 + u_1u_2y_4 + u_1u_3y_5 + u_2u_3y_6 + u_1u_2u_3y_7 \in C^{\perp}$ we have,

$x \cdot y = 0$, according to the Theorem 3.3 we arrive to, $\Phi(x) \cdot \Phi(y) = 0$. Then,

$$\Phi(C^{\perp}) \subseteq [\Phi(C)]^{\perp}. \tag{5}$$

Moreover by Theorem 3.2, we get,

$$|\Phi(C^{\perp})| = |\,[\Phi(C)]^{\perp}\,|. \tag{6}$$

Equation (5) and (6) give,

$$\Phi(C^{\perp}) = [\Phi(C)]^{\perp}.$$

The proof of the second part of the theorem is clear. ■

Theorem 4.4: Let $C = \xi_0 C_0 \oplus \xi_1 C_1 \oplus \xi_2 C_2 \oplus \xi_3 C_3 \oplus \xi_4 C_4 \oplus \xi_5 C_5 \oplus \xi_6 C_6 \oplus \xi_7 C_7$. be a linear code of length n over $\mathcal{A}_{(q,3)}$. Then, $C^{\perp} = \xi_0 C_0^{\perp} \oplus \xi_1 C_1^{\perp} \oplus \xi_2 C_2^{\perp} \oplus \xi_3 C_3^{\perp} \oplus \xi_4 C_4^{\perp} \oplus \xi_5 C_5^{\perp} \oplus \xi_6 C_6^{\perp} \oplus \xi_7 C_7^{\perp}$. Further, C is self-dual if and only if $C_0, C_1, C_2, C_3, C_4, C_5, C_6, C_7$ are self-duals.

Proof.

Let $C^{\perp}$ be a linear code over $\mathcal{A}_{(q,3)}$. If,

$\overline{C}_0 = \{x_0 + x_1 + x_2 + x_3 + x_4 + x_5 + x_6 + x_7, \exists x_0, x_1, x_2, x_3, x_4, x_5, x_6, x_7 \in \mathbb{Z}_q, \text{ such as } x \in C^{\perp}\}$,

$\overline{C}_1 = \{x_0 + x_1 + x_2 - x_3 + x_4 - x_5 - x_6 - x_7, \exists x_0, x_1, x_2, x_3, x_4, x_5, x_6, x_7 \in \mathbb{Z}_q, \text{ such as } x \in C^{\perp}\}$,

$\overline{C}_2 = \{x_0 + x_1 - x_2 - x_3 - x_4 - x_5 + x_6 + x_7, \exists x_0, x_1, x_2, x_3, x_4, x_5, x_6, x_7 \in \mathbb{Z}_q, \text{ such as } x \in C^{\perp}\}$,

$\overline{C}_3 = \{x_0 + x_1 - x_2 + x_3 - x_4 + x_5 - x_6 - x_7, \exists x_0, x_1, x_2, x_3, x_4, x_5, x_6, x_7 \in \mathbb{Z}_q, \text{ such as } x \in C^{\perp}\}$,

$\overline{C}_4 = \{x_0 - x_1 + x_2 + x_3 - x_4 - x_5 + x_6 - x_7, \exists x_0, x_1, x_2, x_3, x_4, x_5, x_6, x_7 \in \mathbb{Z}_q, \text{ such as } x \in C^{\perp}\}$,

$\overline{C}_5 = \{x_0 - x_1 - x_2 + x_3 + x_4 - x_5 - x_6 + x_7, \exists x_0, x_1, x_2, x_3, x_4, x_5, x_6, x_7 \in \mathbb{Z}_q, \text{ such as } x \in C^{\perp}\}$,

$\overline{C}_6 = \{x_0 - x_1 + x_2 - x_3 - x_4 + x_5 - x_6 + x_7, \exists x_0, x_1, x_2, x_3, x_4, x_5, x_6, x_7 \in \mathbb{Z}_q, \text{ such as } x \in C^{\perp}\}$,

$\overline{C}_7 = \{x_0 - x_1 - x_2 - x_3 + x_4 + x_5 + x_6 - x_7, \exists x_0, x_1, x_2, x_3, x_4, x_5, x_6, x_7 \in \mathbb{Z}_q, \text{ such as } x \in C^{\perp}\}$ where x is defined in Equation (2). Then,

$C^{\perp} = \xi_0 \overline{C}_0 \oplus \xi_1 \overline{C}_1 \oplus \xi_2 \overline{C}_2 \oplus \xi_3 \overline{C}_3 \oplus \xi_4 \overline{C}_4 \oplus \xi_5 \overline{C}_5 \oplus \xi_6 \overline{C}_6 \oplus \xi_7 \overline{C}_7$.

It is clear that $\overline{C}_i \subseteq C_i^{\perp}$ for $i = \overline{0,7}$ moreover, if we take $x \in C_i^{\perp}$, for $i = \overline{0,7}$ implies that $x \cdot y = 0, \forall y \in C_i$.

If, $\overline{x} = \xi_0(\overline{x}_0 + \overline{x}_1 + \overline{x}_2 + \overline{x}_3 + \overline{x}_4 + \overline{x}_5 + \overline{x}_6 + \overline{x}_7) + \xi_1(\overline{x}_0 + \overline{x}_1 + \overline{x}_2 - \overline{x}_3 + \overline{x}_4 - \overline{x}_5 - \overline{x}_6 - \overline{x}_7) + \xi_2(\overline{x}_0 + \overline{x}_1 - \overline{x}_2 - \overline{x}_3 - \overline{x}_4 - \overline{x}_5 + \overline{x}_6 + \overline{x}_7) + \xi_3(\overline{x}_0 + \overline{x}_1 - \overline{x}_2 + \overline{x}_3 - \overline{x}_4 + \overline{x}_5 - \overline{x}_6 - \overline{x}_7) + \xi_4(\overline{x}_0 - \overline{x}_1 + \overline{x}_2 + \overline{x}_3 - \overline{x}_4 - \overline{x}_5 + \overline{x}_6 - \overline{x}_7) + \xi_5(\overline{x}_0 - \overline{x}_1 - \overline{x}_2 + \overline{x}_3 + \overline{x}_4 - \overline{x}_5 - \overline{x}_6 + \overline{x}_7) + \xi_6(\overline{x}_0 - \overline{x}_1 + \overline{x}_2 - \overline{x}_3 - \overline{x}_4 + \overline{x}_5 - \overline{x}_6 + \overline{x}_7) + \xi_7(\overline{x}_0 - \overline{x}_1 - \overline{x}_2 - \overline{x}_3 + \overline{x}_4 + \overline{x}_5 + \overline{x}_6 - \overline{x}_7) \in C$.

Then, $\xi_0 x \cdot \overline{x} = 0$ so, $\xi_0 x \in C^{\perp}$ but the code $C^{\perp}$ is unique i.e. d, $x \in \overline{C}_i$. Finally we find, $\overline{C}_i = C_i^{\perp}$, for $i = \overline{0,7}$ and,

$C^{\perp} = \xi_0 C_0^{\perp} \oplus \xi_1 C_1^{\perp} \oplus \xi_2 C_2^{\perp} \oplus \xi_3 C_3^{\perp} \oplus \xi_4 C_4^{\perp} \oplus \xi_5 C_5^{\perp} \oplus \xi_6 C_6^{\perp} \oplus \xi_7 C_7^{\perp}$.

After the self duality of the code C and Theorem 4.1 we have,

$$\begin{aligned} C^{\perp} = C \quad &\Leftrightarrow \quad \Phi\left(C^{\perp}\right) = \Phi\left(C\right) \\ &\Leftrightarrow \quad C_0^{\perp} \otimes \ldots \otimes C_7^{\perp} = C_0 \otimes \ldots \otimes C_7 \\ &\Leftrightarrow \quad C_i^{\perp} = C_i, \text{ for } i = \overline{0,7} \end{aligned}$$

Therefore, C_i for $i = \overline{0,7}$ are self duals.

■

V. Conclusion

This paper is devoted to construction of codes over $\mathcal{A}_{q,3} = \mathbb{Z}_q + u_1\mathbb{Z}_q + u_2\mathbb{Z}_q + u_3\mathbb{Z}_q + u_1u_2\mathbb{Z}_q + u_1u_3\mathbb{Z}_q + u_2u_3\mathbb{Z}_q + u_1u_2u_3\mathbb{Z}_q$. It is obtained by a representation of a linear code of length n over $\mathcal{A}_{q,3}$ by means of $C_0, C_1C_2, C_3, C_4, C_5, C_6$ and C_8 which are linear codes of length n over $\mathbb{Z}_q$.

References

[1] K. Chatouh, K. Guenda, T. A. Gulliver and L. Noui, *Simplex and MacDonald codes over R_q*, J. Appl. Math. Comput. DOI 10.1007/s12190-016-1045-4, 2016.

[2] K. Chatouh, *In-Depth Study of the Homogeneous Weight on $\mathcal{R}_{p^s,\theta} = \mathbb{F}_{p^s} + u_1\mathbb{F}_{p^s} + \ldots + u_\theta\mathbb{F}_{p^s}$ and A New Presentation of Some Linear Codes over this Ring* , Under review, 2018.

[3] Irwansyah, A. Barra, I. Muchtadi-Alamsyah, A.Muchlis, and D. Suprijanto, *Skew-cyclic codes over B_k*, Journal of Applied Mathematics and Computing, DOI 10.1007/s12190- 017-1095- 2.

[4] H. Islam and O. Prakash, *Skew constacyclic codes over $F_q+uF_q+vF_q$*, arXiv:1710.07789v3 [cs.IT] 8 Dec 2017.

[5] , X.Zheng and B.Kong, *Cyclic codes and $\lambda_1 + \lambda_2 u + \lambda_3 v + \lambda_4 uv$-constacyclic codes over $\mathbb{F}_p + u\mathbb{F}_p + v\mathbb{F}_p + uv\mathbb{F}_p$*, Applied Mathematics and Computation 306, pp.86-91, 2017.

An Improved Encryption Approach Based on Multi-chaotic Maps Applied to Digital Image

Lamiche Chaabane
Computer science department,
Mohamed Boudiaf university
M'sila-Algeria
lamiche07@gmail.com

***Abstract*:** With the great acceleration in development of Internet and communication technologies, image communication is a kind that enforces itself strongly and plays a very important role in information transmission. However, information security is a sensitive subject for research, discussion and development, and encryption is one of the best alternatives that has proven to be effective throughout history to ensure the confidentiality and security of information. In this paper, we propose an encryption algorithm for the grayscale image. The developed approach is based on the Hybridization between chaotic logistic maps, chaotic sine maps, and chaotic standard maps, modified Fibonacci sequence, and permutation techniques. Numerical results show the potent of the proposed encryption model to produce better security compared to results given by other literature works

Keywords: Internet, information security, encryption algorithm, decryption, chaotic logistic map, chaotic sine map, chaotic standard map, Fibonacci modified sequence, permutation.

1. Introduction

The great acceleration and the fascinating developments in digital image processing and network communications technologies have made life easy and at the same time added complexity to the world of security. It is necessary to protect the communicated image information against illegal usage, especially for those requiring reliable, fast and robust secure systems to store and transmit, such as military image databases, confidential video conference, medical imaging system, online private photograph album, etc [1].

Encryption is the process of information transformation for securing the data [2][3]. Most of the available encryption techniques were designed only for textual data [4]. There are various encryption algorithms such as DES, AES, RC4 which comes under symmetric encryption algorithms whereas RSA algorithm, which is an asymmetric encryption algorithms [5][6]. However, these algorithms are not suitable for image applications due to some features of images such as redundancy and huge capacity of data [7]. Security of digital images has attracted many in recent years and various encryption methods for images has been proposed to enhance the image security such as chaos-based [8][9][10][11] and Fibonacci techniques [12][13] and permutation techniques[14][15][16]. In this paper, the proposed algorithm scheme consists of three steps. The first step is hiding the plain image bits with the bits of the pseudo-random key stream generated through the exclusive-OR operation (or XOR), the pseudo-random key stream is generated by a chaotic generator of the chaotic standard map used for the choice between two generators (the first one generator is chaotic sine map and the second is modified Fibonacci sequence generator). The second step consists in using pixel and block permutation techniques with a random generated key. The last step is the same as the first but with a change of Fibonacci generator by chaotic logistic map generator.

2. Proposed Method

The proposed image encryption algorithm scheme is decomposed in three parts: (1) pseudo-random keys stream generator. (2) Encryption function. (3) Decryption function.

2.1. Pseudo-random keys stream generator

The pseudo-random keys (key1 and key2) generators are realized by: a chaotic generator of the chaotic standard map used for the choice between two generators (the first generator is chaotic sine map generator and the second is modified Fibonacci sequence generator) for key1, a chaotic generator of the chaotic standard map used for the choice between two generators (the first generator is chaotic sine map and the second is chaotic logistic map generator) for key2.

Key1 generator :

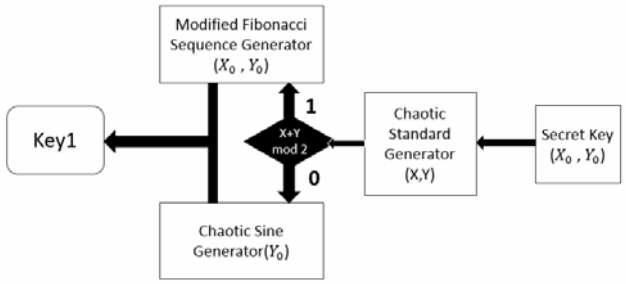


Figure 1: The pseudo-random key1 generator.

Key2 generator :

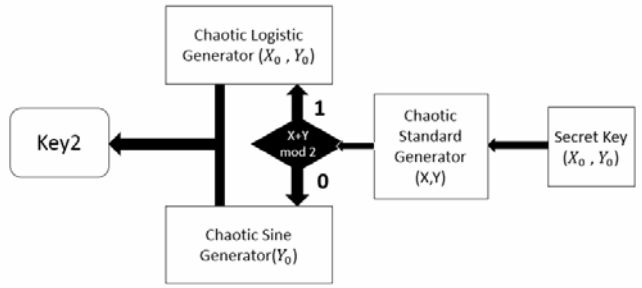


Figure 2: The pseudo-random key2 generator.

Which use the mathematical formulas are as follows:

1) Chaotic sine map pseudo-random number generator

$$Y_{n+1} = \lambda \sin(\pi Y_n)$$

The initial parameters are: (λ, Y).

2) Chaotic logistic map pseudo-random number generator :

$$X_{n+1} = \mu X_n (1 - X_n)$$

The initial parameters are (μ, X).
Where, $0 < \mu \leq 4$ and $0 < X \leq 1$.

3) Chaotic standard map pseudo-random number generator **:**

$$X_{n+1} = X_n + K \sin(Y_n)$$

$$Y_{n+1} = Y_n + X_{n+1}$$

The initial parameters are: (Y, X, K).

4) Modified Fibonacci sequence generator :

$$U_n = (U_{n-1} + U_{n-2}) \, Mod \, M \, , n \geq 2$$

Initial parameters are:
(U_0=$(X_0 \times M) Mod \, M$), (U_1=$(Y_0 \times M) Mod \, M$),
And M = 256.

2.2. Encryption function

The following steps are used to encrypt images :

i. Step 01 : Encryption using key1

1) Generate a pseudo random keys stream:
   A. Set the initial parameters (λ, Y), (μ, X) and (K).
   B. Generate three streams of pseudo-random number, (K_1) from chaotic logistic map, (K_2) from modified Fibonacci sequence and (K_3) from chaotic sine map. Both with same size of the plain image *W* x *H*.
   C. Convert each value from K_1 and K_3 to integer value by K_1 * 256 and K_3 * 256
   D. Generate the two pseudo-random keys streams key1 and key2 from K_1, K_2 and K_3
   E. Convert the two generated keys (key1), (key2) as bits.
2) Convert the plain image to a data stream as bits (m_i).
3) Performing the operation XOR bit by bit between the data stream (the plain image) and the pseudo-random key stream. To obtain a stream of encrypted data (image C_i)
   $C_i = m_i \oplus$ key1.

ii. Step 02 : encryption using Permutation techniques

1) Take a null key (key-permutation), in the end of this step this key will consist of 24 characters
2) Pixel permutation : Choose a character *c* randomly and add it to the (key-permutation) and take its value *Vc* as a parameter to apply a pixel permutation and our pixel permutation algorithm is the follow :

```
For i=0 to width
For j=0 to height
{
image_output[i][j]=image[(i+Vc)Mod(width)][(j+
Vc*2) Mod(height)];
}
```

3) Apply pixel permutation on the image (C_i)
4) Split the image (C_i) into four blocks.
5) Split each block into four sub-blocks
6) Apply pixel permutation on the 16 sub-blocks
7) Split each sub-block into four other sub-blocks

Note: For an image of 04 blocks, there is 4! (24) Permutation possible.

8) Apply a block permutation for each sub-blocks randomly (16 cases) each permutation form has its own code (character), and add the 16 characters to the key-permutation
9) Apply a block permutation for each block randomly (4 cases) each permutation form has its own code (character), and add the 4 characters to the key-permutation
10) Apply a block permutation on the image and add 1 character to the key-permutation
11) Rows and columns shifting : Choose two characters *c_row* and *c_columns* randomly and add them to the (key-permutation) and take theirs values *Vc* and *Vr* as a parameters to apply rows and columns shifting algorithm as follow :

Columns:

```
Cpt=0, col=0;
For i=0 to width
{
If (col< width)
{
For j=0 to height
{
image_output[i][j]=image[col][j];
}
col+=Vc;
}
Else
{
Cpt++;
i--;
col=Cpt;
}
}
```

rows:

```
Cpt=0, rw=0;
For j=0 to height
{
If (rw< height)
{
For i=0 to width
{
image_output[i][j]=image[i][rw];
}
rw+=Vr;
}
Else
{
Cpt++;
j--;
rw=Cpt;
}
}
```

12) Now we have the image C_j the output of step 02 and the key-permutation with 24 characters

iii. Step 03 : Encryption using key2

1) Convert the image C_j to a data stream as bits
2) Performing the operation XOR bit by bit between the data stream (C_j) and the pseudo-random key stream. To obtain a stream of encrypted data (encrypted image C_f) $C_f = C_j \oplus$ key2.

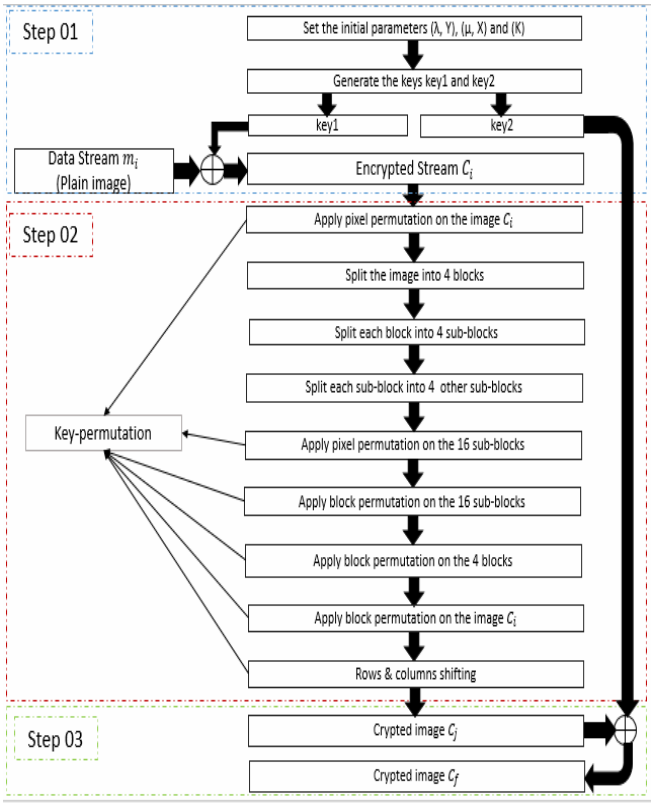


Figure 3 : Block diagram of the encryption function.

2.3. Decryption function

Decryption also consists of three steps but in reverse order, the initial parameters (λ, Y), (μ, X) and (K) with the permutation key must be the same where used in encryption function, and generation of the keys is the same.

Our input is the encrypted image C_f.

i. Step 01 : Decryption using key2

$C_j = C_f \oplus$ key2

ii. Step 02 : Decryption using the reverse permutation

1) Rows and columns shifting with the reverse algorithm and the reverse order
2) Apply the reverse block permutation on the image (C_j)
3) Split the image (C_i) into four blocks
4) Apply the reverse block permutation on the blocks
5) Split each block into four sub-blocks
6) Split each sub-block into four other sub-blocks
7) Apply the reverse block permutation on the sub-blocks
8) Apply the reverse pixel permutation on the 16 sub-blocks
9) Apply the reverse pixel permutation on the image C_j
10) Now we have the image C_i the output of step 02

iii. Step 03: Decryption using key1

$m_i = C_i \oplus$ key1.

m_i is the plain image

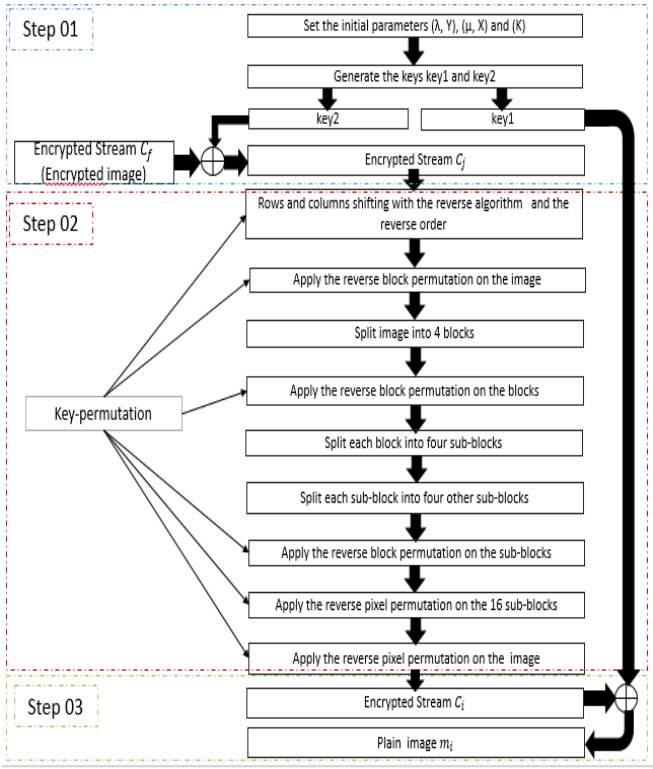


Figure 4 : Block diagram of the decryption function.

3. Experimental Results

A good encryption procedure should be robust against all kinds of cryptanalytic, statistical and brute-force attacks. In this section, key space analysis, Histogram, information entropy and correlation coefficient analysis were carried out to clarify the good performance of the proposed model.

3.1 Image database

The database image used in this paper is free available in University of Southern California [17], University of Waterloo [18], and University of Wisconsin-Madison [19].Witch primarily support research in image processing, image analysis, and machine vision.

3.2 Key space Analysis

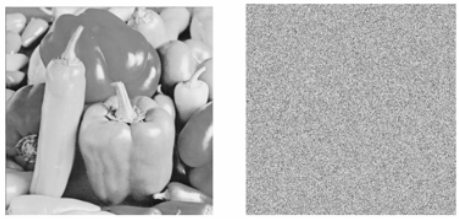
For a secure image cipher, the key space should be large enough to make the brute force attack infeasible. The size of the key may be longer than the size of the The image. In the proposed encryption technique, Key space is the total number of different keys used in the procedure composed of six parts (λ, Y, μ, X, K) and the permutation key (24 characters), without constraints, the size of key space is:

$$(2^{64})^5 \times (2^8)^{24} = 2^{512}$$

The key space is large enough because this number represented in 512 bits.

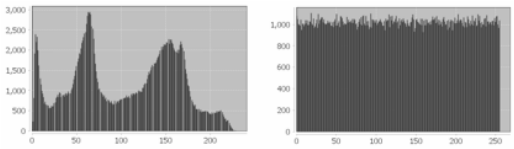
3.3 Histogram Analysis

The histogram of the ciphered image should be significantly different from the histogram of the plain image, and the histogram of the ciphered image should be as uniformed distribution as possible that will indicates more randomness [20][21]. For the histogram analysis, we used grayscale image (peppers.tiff) with size of 512 × 512.



(a) *(b)*

Figure 5: (a) Plain image; (b) Encrypted image.



(a) Plain image *(b) Encrypted image*

Figure 6: *Histograms of images.*

3.4 Entropy Correlation Coefficient Analysis

Entropy states the degree of uncertainty in a system. It can be done as follows:

$$H(m) = -\sum_{i=0}^{2^n-1} p_i \log_2(p_i)$$

Where: n is the number of bits to encode pixels.

For images with random pixels, which are encoded by 8 bit, entropy should be equal to 8. However, entropy is usually smaller than 8, but a value closer to eight means that the possibility of predictability is less and the security level is higher [22][23].

Correlation is a statistical technique that can show whether and how strongly pairs of variables are related. The correlation coefficients are calculated by the following equation for two variables x and y of length N [24]:

$$r = \frac{cov(x,y)}{\sqrt{D(x)}\sqrt{D(y)}}$$

Where:

$$cov(x,y) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))(y_i - E(y))$$

$$E(x) = \frac{1}{N}\sum_{i=1}^{N} x_i$$

$$D(x) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))^2$$

For images, we randomly select pairs of two-adjacent pixels from plain images and ciphered images, and calculate the correlation coefficients, respectively by using the equations cited above. If the correlation is closer to 0 that means better encryption effect.

For the test case, we used grayscale images, like lena, peppers and some other images, In addition to making comparison with other recent works in the entropy coefficient, and the initial parameters are the follows : (λ=3.89, Y=0.9, μ=3.9, X=0.9, K=18.9), and the permutation-key = "qucnslmhaahjhrgoahagoHHn"

Table 1: Entropy and correlation coefficient.

Input images	Size	Encrypted image entropy	Encrypted image correlation coefficients
5.1.09.tiff	256× infofai93@gmail.com	7.9968	0.00202
5.1.11.tiff	256×256	7.9974	0.00096
5.1.12.tiff	256×256	7.9977	0.00057
5.1.14.tiff	256×256	7.9972	-0.00064

5.2.08.tiff	512×512	7.9992	0.00049
5.3.01.tiff	1024×1024	7.9998	-0.00069
5.3.02.tiff	1024×1024	7.9998	0.00081
7.1.07.tiff	512×512	7.9992	-0.00003
boat.512.tiff	512×512	7.9993	0.00039
elaine.512.tiff	512×512	7.9993	0.00060
lena.tiff	512×512	7.9992	-0.00219
peppers.tiff	512×512	7.9992	0.00161
barbara.tiff	512×512	7.9993	0.00096
Cameraman.tiff	256×256	7.9974	-0.00133
Testpat.1k.tiff	1024×1024	7.9997	0.00030
Average		**7.9987**	**0.00090**

Table 2: The comparison of entropy coefficient.

Input images	Our approach	Ref. [11]	Ref. [25]
5.1.09.tiff	7.9968	7.9975	7.9987
5.1.11.tiff	7.9974	7.9972	7.9974
5.1.12.tiff	7.9977	7.9975	7.9992
5.1.14.tiff	7.9972	7.9971	7.9964
5.2.08.tiff	7.9992	7.9993	7.9976
5.3.01.tiff	7.9998	7.9998	7.9975
5.3.02.tiff	7.9998	7.9998	7.9960
7.1.07.tiff	7.9992	7.9994	7.9969
boat.512.tiff	7.9993	7.9993	7.9980
elaine.512.tiff	7.9993	7.9992	7.9985
lena.tiff	7.9992	7.9991	7.9963
peppers.tiff	7.9992	7.9992	7.9985
barbara.tiff	7.9993	7.9993	7.9978
Cameraman.tiff	7.9974	7.9972	7.9985
Testpat.1k.tiff	7.9997	7.9998	7.9986
Average	**7.9987**	**7.9987**	**7.9977**

The results show that after simulating 15 images, the average value of the entropy from the encrypted images is 7.9987. It is closer to the value 8. And the average value of correlation coefficients from the encrypted images is 0.0009, which is closer to 0. Which means the effectiveness of our proposed encryption algorithm. In addition, the results of comparison with recent works proved the efficiency of our proposed encryption algorithm.

4. Conclusion

In this paper, we have proposed a hybrid image encryption, which based on combination of chaotic logistic map, chaotic sine map, modified Fibonacci sequence and multiple permutation techniques. The experimental results showed that the proposed image encryption system has a very large key space, and high-level security. Thus, the analysis proves the security, correctness, effectiveness. In addition, the results of the proposed algorithm are particularly suitable for Internet image encryption, transmission applications and communication technologies.

5. References

[1] Ruisong, Y. and Haiying, Z. (2012). An Efficient Chaos-based Image Encryption Scheme Using Affine Modular Maps. I. J. Comp. Net.and Infor. Security, 7, pp.41-50.

[2] Mohammad Ali BaniYounes and AmanJantan, "Image encryption using block-based transformation algorithm", IAENG Int. J. of Computer Science, Vol 35, No.1, 2008.

[3] Sesha Pallavi Indrakanti and Avadhani P.S, "Permutation based image encryption technique", Int. Journal of Computer Applications, Vol. 28, No.8, 2011.

[4] Manju Rani and Sudesh Kumar, "Analysis on different parameters of encryption algorithms for information security", Int. J. of Adv. Res. in Computer Science and Software Engineering", Vol. 5, No. 8, 2015.

[5] William Stallings, "Cryptography and Network Security Principles and Practices", Prentice Hall, New Delhi, 2015.

[6] Bruce Schneier, "Applied Cryptography", John Wiley & Sons, New York, 2010.

[7] Sesha Pallavi Indrakanti and Avadhani P.S, "Permutation based image encryption technique", Int. Journal of Computer Applications, Vol. 28, No.8, 2011.

[8] Tiegang Gao, Zengqiang Chen. A new image encryption algorithm based on hyper-chaos. Physics Letters A, 372(4):394–400, 2008.

[9] Baydda Flaeh AL-Saraji, Mustafa Dhiaa AL-Hassani. Multi-Levels Image Encryption Technique based on Multiple Chaotic Maps and Dynamic Matrix, Int. Journal of Computer Applications: (0975 - 8887) Volume 151, 2016.

[10] G.A.Sathishkumar, Dr.K.Bhoopathy bagan, Dr.N.Sriraam. Image encryption based on diffusion and multiple chaotic maps. International Journal of Network Security & Its Applications (IJNSA), Vol.3, No.2, 2011.

[11] Rim Zahmoul, Ridha Ejbali and Mourad Zaied. Image encryption based on new Beta chaotic maps. Optics and Lasers in Engineering 2017.

[12] Yicong Zhou, Karen Panetta, Sos Agaian, and CL Philip Chen. Image encryption using p-fibonacci transform and decomposition. Optics Communications, 285(5): 594–608, 2012.

[13] Weijia Cao, Yicong Zhou, C.L. Philip Chen. A New Image Encryption Algorithm Using Truncated P-Fibonacci Bit-planes. IEEE Int. Conf. on Systems, Man, and Cybernetics, 2012.

[14] Sesha Pallavi Indrakanti and P.S.Avadhan. Permutation based Image Encryption Technique. International Journal of Computer Applications (0975 – 8887) Volume 28– No.8, August 2011.

[15] Avi Dixit, Pratik Dhruve and Dahale Bhagwan. Image encryption using permutation and rotational XOR technique. SIPM, FCST, ITCA, WSE, ACSIT, CS & IT 06, pp. 01–09, 2012. © CS & IT-CSCP 2012.

[16] G.S.Nandeesh, P.A. Vijaya and M.V. Sathyanarayana. International Journal of Computer Science and Mobile Computing، Vol. 2, Issue. May 2013, pg.145 – 154.

[17] University of Southern California, database image http://sipi.usc.edu/database/database.php?volume=misc

[18] University of Waterloo, image database http://links.uwaterloo.ca/Repository.html

[19] University of Wisconsin-Madison, image database, https://homepages.cae.wisc.edu/~ece533/images/

[20] Zhang Yong, “Image Encryption with Logistic Map and Cheat Image”, International Conference on Computer Re-search and Development, pp [97-101], March 2011.

[21] RashidahKadir, RosdianaShahril, and MohdAizainiMaarof, “A Modified Image Encryption Scheme Based on 2D Chaotic Map”, International Conference on Computer.

[22] Alireza Jolfaei, Abdul Rasoul Mirghadri, “An Image Encryption Approach Using Chaos and Stream Cipher”, Jou. of Theoretical and Applied Infor. Technology, (2010).

[23] Dijana TRALIC, Sonja GRGIC. «Robust Image Encryption Based on Balanced Cellular Automaton and Pixel Separation, 2016

[24] J. S. Fouda, J. Y. Effa, S. Sabat, and M. Ali, “A Fast Chaotic Block Cipher for Image Encryption,” Communications in Nonlinear Science and Numerical Simulation, vol. 19, no. 3, pp. 578–588, 2014.

[25] Akram Belazi, Ahmed A Abd El-Latif, Safya Belghith. A novel image encryption scheme based on substitution-permutation network and chaos. Signal Process 2016;128:155–70. [ISSN 0165-1684].

Secure Hybrid Crypto-system AES/RSA on FPGA for Data Communication

M. Issad, N.Anane, A.M.Bellemou
Centre de Développement des Technologies Avancées, CDTA
Baba Hassen, Alger, Algérie
missad@cdta.dz

B. Boudraa
Université des Sciences et de la Technologie Houari Boumediene,
Bab Ezzouar, Alger, Algerie
b.boudraa@yahoo.fr

Abstract—***with the development of information technologies, our environment is surrounded by digital data that transit via networks. When data are important, they become vulnerable to external attacks which can be avoided by using cryptography which provides confidentiality, integrity and availability required to secure digital data transactions such as e-commerce, mobile telephony and Internet.***
This paper deals with securing data transmitted over a network composed by a server and several clients, where a security platform has been integrated into the server and embedded on an FPGA circuit. The protection of data transfer between clients is provided by hybrid cryptography combining symmetric and asymmetric cryptographies. The security of client-server communication is ensured by the AES protocol and the Diffie-Hellman key exchange protocol. To offer a good management of keys and their sharing, a dedicated system for generating keys is designed to fit with public key infrastructures. This system is a part of the server and has been implemented using JAVA language and executed on a computer. This communication system provides a Graphical User Interface (GUI) offering to clients ease and flexibility in transferring their data.

Keywords— Diffie-Hellman, Hybrid cryptosystem, AES/ RSA, Secure transmission, Virtex-5, FPGA**.**

I. INTRODUCTION

Today, more and more sensitive data is stored digitally. Bank accounts, medical records and personal emails are some categories that data must keep secure; this has made cryptography an important research topic.

Cryptography is the science of using mathematics to encrypt and decrypt data. It enables to store sensitive information or transmit it across insecure networks so that it cannot be read by anyone except the intended recipient. Cryptography is the process that involves encryption and decryption of text using various algorithms based on mathematical functions. These algorithms of encryption/decryption can be categorized into symmetric and asymmetric ones.

In symmetric cryptography, the same key is used by the sender and the receiver and must keep it secret. Asymmetric cryptography requires a pair of keys of large size between each two communicators and poses the problem of key distribution. Current cryptographic systems exploit the strengths of both symmetric and asymmetric cryptographies. Symmetric encryption is preferred when confidentiality is required because it is faster as it uses smaller keys than asymmetric encryption.

To provide security and performance while transmitting data via a network, a hardware/software co-design is a good solution to ensure faster speed, more security and consumes less area and power. The hardware implementation on FPGA, which is reconfigurable, offers more flexibility and requires less time to market. This paper focuses on securing transmitted data via a network infrastructure composed by a server and several clients. Figure 1 shows the Client/Server model architecture that is used in most network systems.

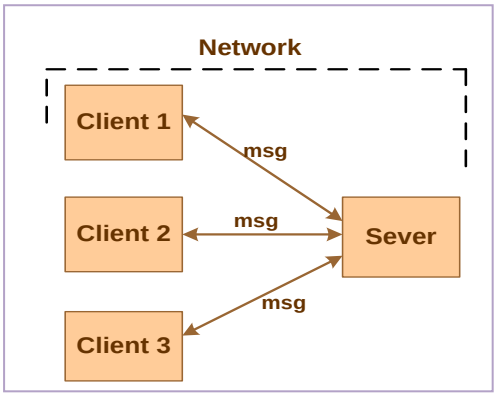


Figure 1. Client/Server architecture

The client side could be any type of smart devices (desktop, laptop, smart phone, etc.). The server part is one device that control and pass messages and opening the connections among clients and/or between clients and server [1]. The Internet part could be one device to isolate the network overall into two main parts: client(s) and server, it could be a switch, a hub, a router or just a cable.

In this paper, we have developed a security platform that has been integrated into the server and embedded on FPGA [2]. The implemented network infrastructure can securely transmit encrypted messages or files via a LAN (Local Area Network) basing on the User Datagram Protocol (UDP) [3], which allows transferring large files across the Internet in real-time with low overhead and less processing. Securing data transfer, between clients, is provided by hybrid cryptography combining symmetric cryptography (AES) and asymmetric cryptography (RSA). The security of the client-server communication is ensured by the

AES protocol and the Diffie-Hellman Key Exchange protocol (DHKE) [4].

This paper is organized as follows: Section II elucidates about cryptography, where the Diffie-Hellman protocol, the cryptographic algorithms AES and RSA and their combination in hybrid cryptosystem are detailed. Section III, presents the proposed hardware architecture for secure transmitting data over a network. Results and discussions are given in section IV. Finally, in Section V, a brief conclusion is drawn.

II. CRYPTOGRAPHYC PROTOCOLS

In the network security system, cryptography plays a vital role for secure transmitting information. Cryptography is a process of integrating and transferring data to users against any attacks. There are two types of cryptographic algorithms: symmetric and asymmetric.

In the symmetric cryptography, shown in figure 2, one secret key is used for both encryption and decryption. The problem with this method is that you have to communicate the secret key securely to your intended recipient. Symmetric algorithms are fast and simple to implement since they use small keys sizes.

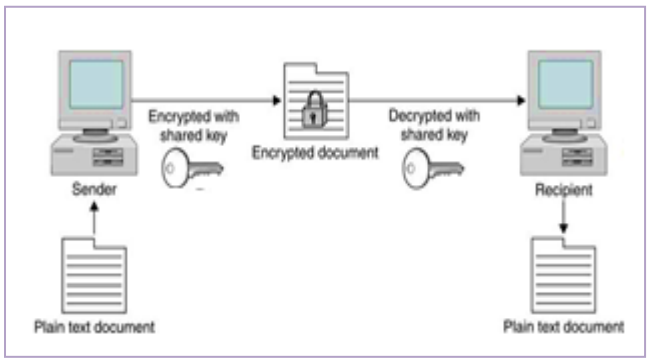


Figure 2. Symmetric Cryptography

Asymmetric cryptography, shown on figure 3, uses a pair of keys: a public key to encrypt the message at sender and a private key known only to receiver for decrypting the encrypted message. Asymmetric algorithms are more secure but require a huge amount of calculus since they use large keys sizes to encrypt the message [5].

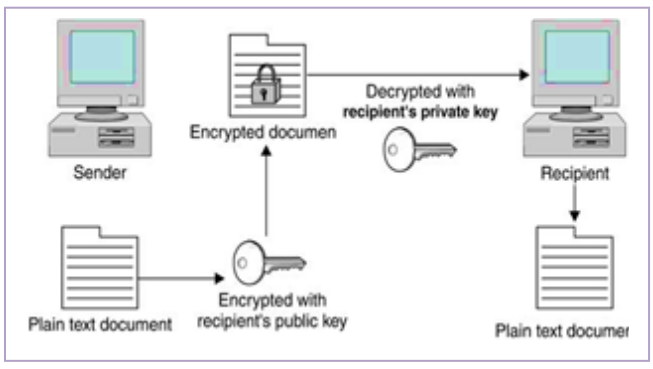


Figure 3. Asymmetric Cryptography

The concept of public key cryptography was introduced by Diffie-Hellman in1976. Their contribution was the notion that keys could come in pairs (encryption and decryption keys) and that one could not generate one key from the other. Since 1976, numerous public key cryptosystems have been proposed and the secure and practical ones are the Diffie Hellman Key exchange (DHKE) and the Rivest Shamir Adleman (RSA).

A. Diffie Hellman Key Exchange protocol

The DHKE is a secure method for exchanging cryptographic keys over an insecure channel. This method allows two parties that have no prior knowledge of each other to jointly establish a shared secret key over an insecure channel. This key can then be used to encrypt subsequent communications using a symmetric key cipher. The simplest implementation of the protocol uses the multiplicative group of integers modulo p, where p is a prime and g is a primitive root modulo p. These two values are chosen in this way to ensure that the resulting shared secret can take on any value from 1 to p–1.

Here is an example represented on figure 4, where A and B agree to use a modulus p and a base g.
A chooses a secret integer "***a***", then sends to B, $A = g^{a} \bmod p$, where B chooses a secret integer "***b***", then sends to A, $B = g^{b} \bmod p$.

- A computes $K = B^{a} \bmod p$
- B computes $K = A^{b} \bmod p$
- A and B now share a secret $K = B^{a} \bmod p = (g^{b} \bmod p)^{a} \bmod p = g^{ab} \bmod p = (g^{a} \bmod p)^{b} = A^{b} \bmod p$.

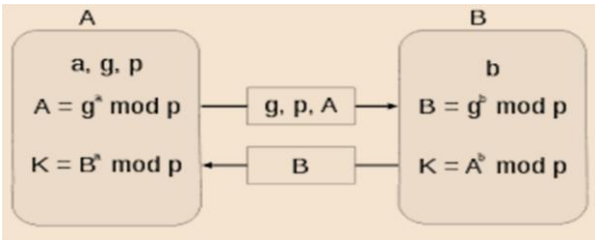


Figure 4. Diffie Hellman key exchange protocol

B. RSA Cryptosystem

The RSA crypto system, shown on figure 5, was called for their inventors named: ***R***onald Rivest, Adi ***S***hamir, and Leonard ***A***dleman. It is a public key encryption algorithm developed for signing and encrypting. It is still widely used in electronic commerce protocols, and is believed that its security depends on the difficulty of decomposing large numbers. RSA is secure because it is able to resist concerted attack and is based on modular exponentiation of large sizes integers.

The computational steps for key generation of RSA are described in the following steps [6]:

1. Generate two different primes p and q of the same length.
2. Calculate the modulus $n = p \times q$.
3. Calculate the quotient $\varphi(n) = (p - 1) \times (q - 1)$.
4. Select for public exponent an integer e such that:

$$1 < e < \varphi(n) \text{ and } \gcd(\varphi(n), e) = 1.$$

5. Calculate for the private exponent a value for d such that:

$$d = (e^{-1}) \bmod \varphi(n).$$

6. Public Key = {e, n}. Private Key = {d, n}.
7. Encrypting a message m is computing $c = m^{e} \bmod n$
8. Decrypting the message c is computing $m = c^{d} \bmod n$.

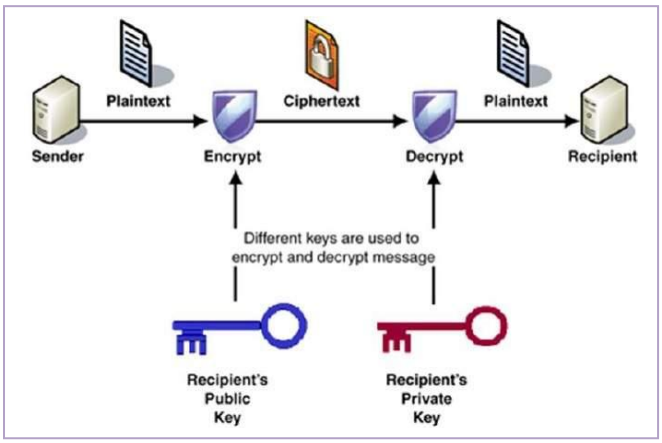


Figure 5. RSA crypto system

C. Advanced Encryption Standard

Advanced Encryption Standard (AES) NIST (2001), is an algorithm used for data encryption. AES is a part of the symmetric block cipher family, which is working with blocks of data, and they are of fixed length (128 bits). These bits are placed to matrix of 4×4, when one cell of matrix corresponds to one byte. One key of length 128, 192 or 256 bits is used for encryption and decryption. In this paper we are working with 128 bits key. This algorithm is shown on figure 6.

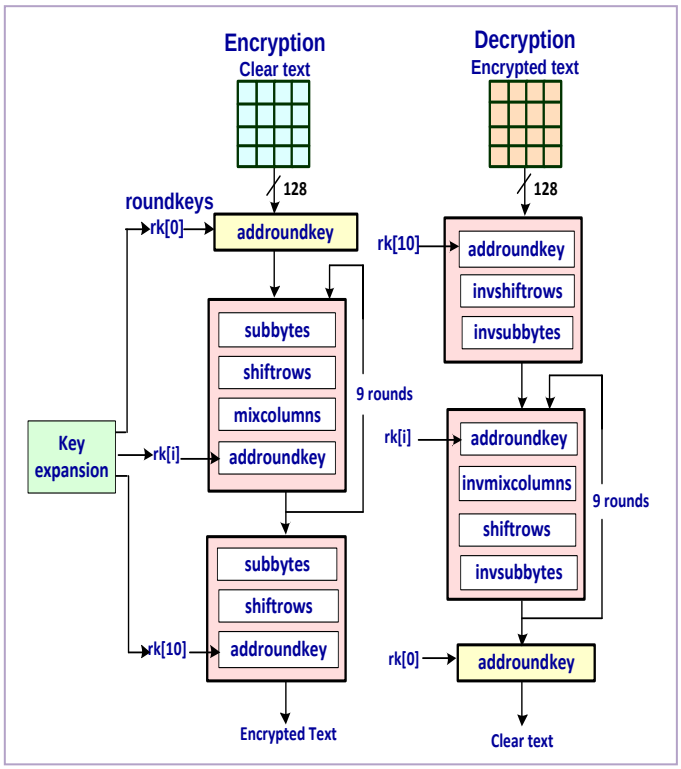


Figure 6. AES Algorithm

The AES cryptosystem can be divided into three parts [7]:

- Initial part (Key Expansion, AddRoundKey),
- Iteration part– so called round (SubBytes, ShiftRows, MixColumns, AddRoundKey),
- Final part (SubBytes, ShiftRows and an AddRoundKey).

An expansion of the key is performed at the beginning of the encryption. In the cipher XOR operation between the 128 bits key and the 4×4 state matrix (block of 128 bits of data) is performed. Subsequently, nine iterations which are normally referred to as the round are performed. The number of rounds depends on the length of the key, for 128 bits key it is 9. Every round consists of the substitution of the bytes in the state matrix (Sub Bytes), rotation of rows (Shift Rows), and substitution of columns (Mix Columns).

The matrix is combined with round's key (Add Round Key), at the end of each round. The final part consists of the substitution of the bytes, rotation of rows and the last addition of the round key. Bytes of the cipher text are stored in the resulting matrix

D. Hybrid Cryptosystem

Symmetric and asymmetric cryptosystems have their own advantages and disadvantages. Symmetric cryptosystems are significantly faster than asymmetric ones, but require all parties to somehow share a secret (the key). Asymmetric cryptosystems are secure and allow public key infrastructures and key exchange systems, but at the cost of speed since they use big size keys hence require a huge amount of calculus .

A hybrid cryptosystem combines the symmetric and asymmetric cryptographies in order to benefit from the rapidity of one and the security of the other. It offers better efficiency and performance.

The hybrid cryptosystem is shown in Figure 7, which consists in generating a random secret key for a symmetric cipher, and then encrypting this key via an asymmetric cipher using the recipient's public key. The message itself is then encrypted using the symmetric cipher and the secret key. Both the encrypted secret key and the encrypted message are then sent to the recipient.

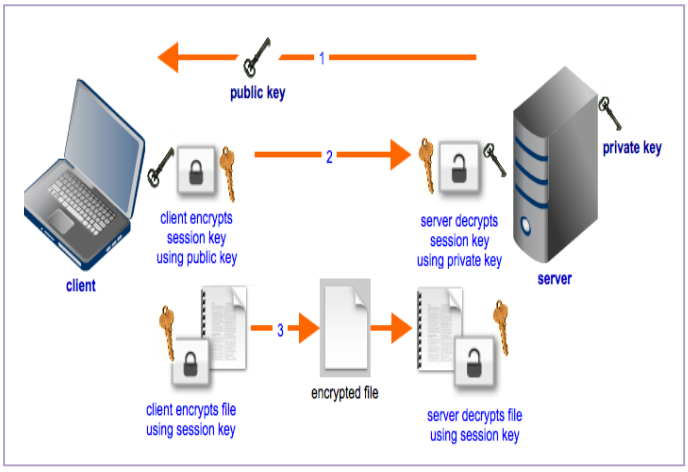


Figure 7. Hybrid cryptography

Hybridization deploys the convenience of the public-key cryptosystem RSA and the efficiency of the private key cryptosystem AES.

AES is usually high speed and requires low RAM, so it is very useful for encrypting data, but since it's the same key for both encryption and decryption, there is a big problem of key transport from the encryption side (sender) to the decryption side (receiver). RSA is used to protect the encryption key by generating two keys (private and public). The private key stays on the receiver side and the public key is sent to the sender side. The sender will use this key to encrypt data.

III. THE PROPOSED ARCHITECTURE

The architecture of our security infrastructure is shown on figure 8. The proposed platform is dedicated to transmit data securely via a LAN and is implemented on an FPGA circuit. It is based on hybrid cryptographic protocols combining AES, RSA and the Diffie-Helleman key exchange protocol. This design is composed by two parts: the server and clients where their communication is based on the UDP protocol. It is composed of the server and clients linked by an Ethernet communication.

A. The server

It is composed of two sub-parts connected by an RS232 link.

1. An FPGA prototyping card embedding a security platform which roles are:
   - Computation of the modular exponentiation required by the DHKE protocol for the creation of secure server-client channel.
   - AES encryption/decryption on the server.
   - Data emission/reception between clients via an Ethernet link.
   - Data emission/reception with the IHM server via the RS232 serial link.
2. An RSA key generator and a database, which roles consist in:
   - Generating random numbers used in the DHKE protocol.
   - Generating RSA public and private keys associated to each client.
   - Transmitting Data to the FPGA circuit.
   - Receiving IDs clients and storing them in the database.
   - Displaying the database.

B. The client

The client part concerns the IHM which tasks are:

- Generating of a random number used in the DHKE.
- AES encrypting/decrypting during server-client and client-client communications.
- RSA encrypting/decrypting during client-client communication.
- Transmitting/receiving data to the part implemented on the FPGA circuit via the Ethernet link.
- Transmitting/receiving data between clients via Ethernet link and displaying data received in clear.

This IHM offers to users a flexible use with the following options:

- Registration of the client who requests to be added to the database.
- Connection of the client who wants to be connected to the infrastructure.
- Sending a message from one client to another.
- Login out of the client from the infrastructure.

The designed infrastructure ensures secure communications between several communicating clients around the server. This security is provided by either encryption / decryption of data transmitted in real time, or by transmission of files stored in the internal memory of the client computer. The functionality of this infrastructure is structured as shown on figure 8.

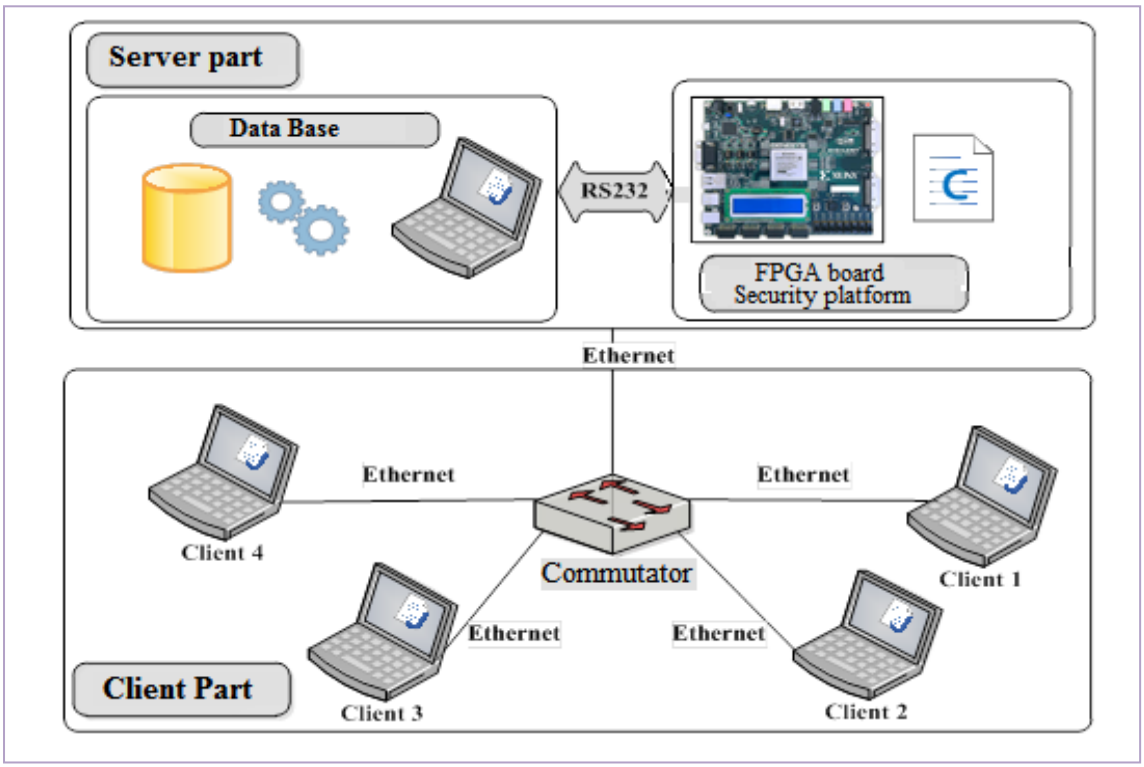


Figure 8. Secure infrastructure architecture

The communication process using the proposed infrastructure is composed by several tasks accomplished by the server, the client C_i and another client C_k. These tasks are numbered from 1 to 11 and executed in the numbering order as shown on figure 9.

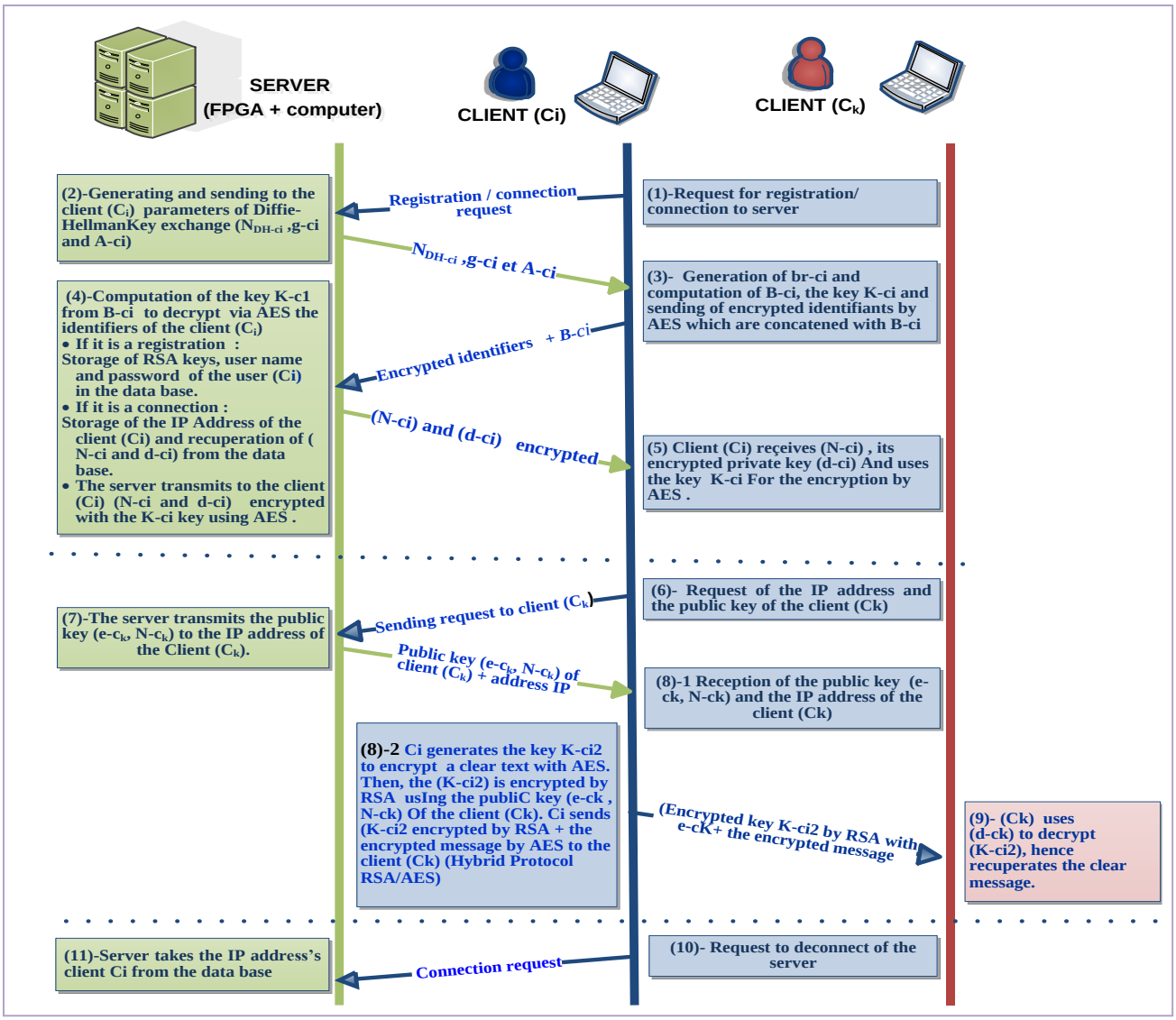


Figure 9. Communications Client-Server and Client-Client

IV. IMPLEMENTATION RESULTS

To conceive the server-client infrastructure, two tasks have been executed:

1. Hardware implementation of an embedded crypto system by using XPS (Xilinx Platform Studio) and its programming in C language by using SDK (Software Development Kit.
2. Creation of an IHM for the client and a data base using JAVA of Netbeans.

Performances of the embedded cryptosystem on the FPGA circuit (the XCVLX50T) concern the execution time of the AES encryption/decryption represented by (t_{AES}), the computation time of a modular exponentiation for a 128-bits exponent represented by (t_{exp}) and the occupied hardware resources.

The execution performances are evaluated using a frequency of 100 MHz. The obtained results are shown in Table 1.

Table 1. Execution performances on FPGA circuit

Execution time			Occupied area		
t_{AES} (encrypt)	t_{AES} (decrypt)	t_{exp}	Slices	Memory blocks	DSP blocks
0.19 ms	0.34 ms	8.5 ms	1323	18	3

The developed interface offers to the user the following tasks:

1. *Secure clients' connection to the server.*

   To connect to the server, the user authenticates by his username and his password which are encrypted by the AES protocol.

When the server does not recognize the client, it asks him to create a new account as shown on figure 10.

Figure 10. Authentication window

2. Secure clients registration in the database server.

The client registers on the server in order to be added to the database using his username and his password. If his username is already stored in the database, the server asks him to change it as shown on figure 11.

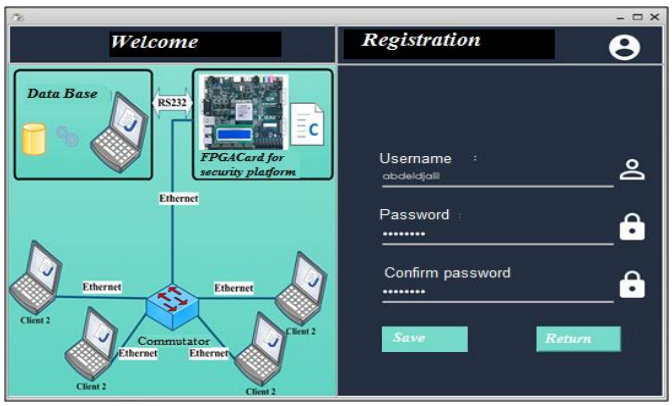


Figure 11. Clients Registration window

3. Secure communication in real time between two clients.

Once clients are registered or connected, they can communicate by transmitting and receiving information (files) between them as shown on figure 12 and 13.

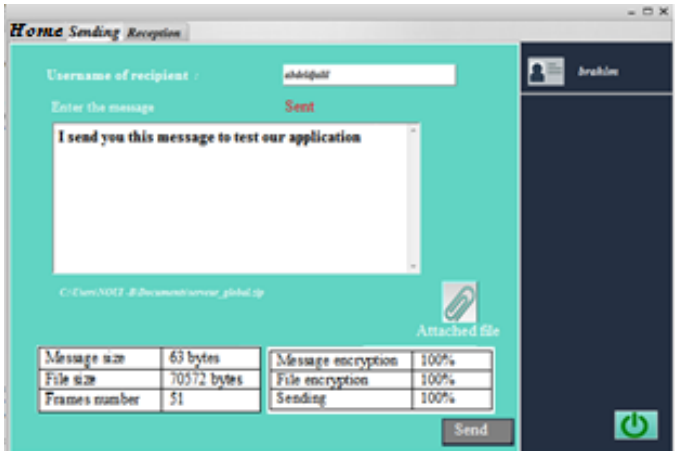


Figure 12. Data sending window

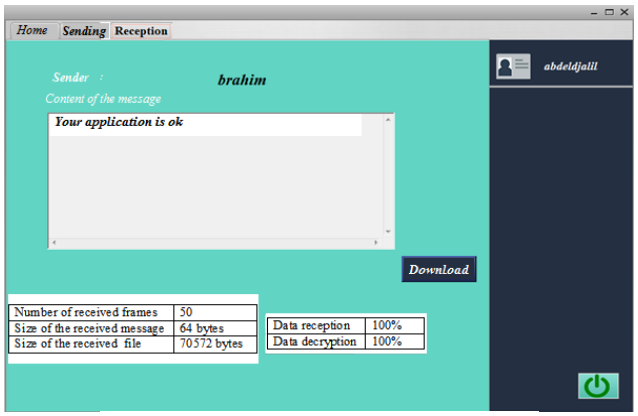


Figure 13. Data reception window

V. CONCLUSION

This paper has presented a security infrastructure based on hybrid crypto system AES/RSA embedded on FPGA circuit. This application can be used to transmit messages and encrypt files securely over a LAN.

Experimental results have shown that the developed security infrastructure exhibits obvious speed and performance advantages in comparison with related works and offers more security.

Our security infrastructure can be considered as a first prototype, where all the critical operations are embedded on FPGA circuit.

In perspective, this work can be improved by the integration of a random number generator on the part implemented on FPGA circuit [8].

Acknowledgement

The authors would like to thank the Directorate General for Scientific Research and Technological Development of Algeria for funding this work through research.

REFERENCES

[1] Ferdi SÖNMEZ, Jalal Sadoon Hameed Al-Bayati, "Development Of A Client / Server Cryptography-Based Secure Messaging System Using RSA Algorithm" Journal of Management Engineering and Information Technology (JMEIT), Volume -4, Issue- 6, Dec. 2017.

[2] Zodpe, H., Sapkal, A, "An efficient AES implementation using FPGA with enhanced security features", *Journal of King Saud University – Engineering Sciences (2018)*,https://doi.org/10.1016/j.jksues.2018.07.002

[3] Eman Salim Ibrahim Harba, "Secure Data Encryption Through a Combination of AES, RSA and HMAC", *Engineering, Technology & Applied Science Research journal*, Vol. 7, No. 4, 2017, pp. 1781-1785.

[4] Whitfield Diffie and Martin Hellman, "New Directions in Cryptography", *IEEE Transactions on Information Theory*, vol. IT-22, Nov. 1976

[5] Teddy Mantoro, Andri Zakariya, "Securing E-Mail Communication Using Hybrid Cryptosystem on Android-based Mobile Devices", the TELKOMNIKA Journal, Vol.10, No.4, December 2012, pp. 807~814.

[6] David Smekal ,Jakub Frolka, Jan Hajny, "Acceleration of AES Encryption Algorithm Using Field Programmable Gate Arrays", IFAC-Papers OnLine 49-25 (2016) ,pp.384–389, Elsevier.

[7] V. Narasimha Nayak, M. Ravi Kumar, K. Anusha, Ch. Kranthi Kiran, " FPGA based asymmetric crypto system design" , International Journal of Engineering & Technology, 7 (1.1) (2018), pp. 612-617.

[8] Vishakha V. Bond, A. D. Kale "Design and Implementation of a Random Number Generator on FPGA" International Journal of Science and Research (IJSR) Volume 4 Issue 5, May 2015.

On public key cryptosystem based on the word problem in a group

Nacer Ghadbane
Laboratory of Pure and Applied Mathematics, Department of Mathematics, University of M'sila, Algeria
nasser.ghedbane@univ-msila.dz

***Abstract*—One of the classical problems in mathematics is the word problem in a group. The difficulty and complexity for solving this problem is used in most of the cryptosystems.**
For a fixed set of elements $S = \{s_1, ..., s_n\}$ in group G, a word in S is any expression of the sort $s_{i_1}^{k_1} s_{i_2}^{k_2} ... s_{i_n}^{k_n}$ where the exponents k_j are positive or negative integers, and $s_{i_1}, ..., s_{i_n} \in S$.
The word problem in a group G with respect to a subset $S = \{s_1, ..., s_n\}$ is the question of telling whether two words in S are equal. It is known that in general the word problem is undecidable, meaning that there is no algorithm to solve it.
In this paper, we introduce a cryptosystem based on the word problem in a group G.

***Index Terms*—Group, word in a group, Word problem in a group, Combinatorial group theory, Public key cryptography.**

I. Intoduction

The creation of public key cryptography by Diffie and Hellman in 1976 and the subsequent invention of the RSA public key cryptosystem by Rivest, Shamir and Adleman in 1978 are watershed events in the long history of secret communications. Public key cryptography draws on many areas of mathematics, including number theory, abstract algebra, and information theory.

A secure public key cryptosystem requires a mathematical operation which is easy to compute (encryption) but computationally difficult to reverse (decreption) in a realistic time without knowing a special secret information, called the trapdoor, which is the private key.

Recall that if G is a group and $X \neq \emptyset$ a subset of G,

$$gp(X) = \{x_1^{\epsilon_1} ... x_n^{\epsilon_n} : x_i \in X, \epsilon_i \in \{1, -1\}\}$$

If $x_1^{\epsilon_1} ... x_n^{\epsilon_n}$ and $y_1^{\mu_1} ... y_m^{\mu_m}$ are two words with $x_i, y_i \in X$ and $\epsilon_i, \mu_i \in \{1, -1\}$, then they are said to be identytical if $n = m, x_i = y_i$ and $\epsilon_i = \mu_i$ for $i = 1, ..., m$.

The word problem in a group G with respect to a subset $S = \{s_1, ..., s_n\}$ is the question of telling whether two words in S are equal. It is known that in general the word problem is undecidable, meaning that there is no algorithm to solve it.

The remainder of this paper is organized as follows. In Section 2, we begin with some elementary material concerning of group and word problem in a group. In Section 3, we investigate the public-key cryptosystem based on The word problem in a group. Finally, we draw our conclusions in Section 4.

II. Preliminaries

A group is a non-empty set G on which there is a binary operation
$(a, b) \longmapsto ab$ such that

- if a and b belong to G then ab is also in G (closure).
- $a(bc) = (ab)c$ for all a, b, c in G (associativity).
- there is an element $1 \in G$ such that
$a1 = 1a = a$ for all $a \in G$ (identity).
- if $a \in G$, then there is an element $a^{-1} \in G$
such that $aa^{-1} = a^{-1}a = 1$.

A group G is called abelian if the binary operation is commutative, i.e., $ab = ba$ for all $a, b \in G$.

A group $(G, \cdot)$ is finite if it has a finite number of elements. We denote the cardinality or order of the group G by $|G|$.

A subset H of a group G is a subgroup of G, if and only if $H \neq \emptyset$ and $ab \in H, a^{-1} \in H$ for all $a, b \in H$ and
is denoted by $H \leq G$.

If a and b are any two elements of G, we have that $(ab)\left(b^{-1}a^{-1}\right) = abb^{-1}a^{-1} = 1$, whence, by the uniqueness of the inverse, $(ab)^{-1} = b^{-1}a^{-1}$.

In a finite group of order m there are m^2 such products, which may be conveniently listed in a $m \times m$ multiplication table, as was first suggested by A. Cayley [6].

For a fixed set of elements $S = \{s_1, ..., s_n\}$ in group G, a word in S is any expression of the sort

$$s_{i_1}^{k_1} s_{i_2}^{k_2} ... s_{i_n}^{k_n}$$

where the exponents k_j are positive or negative integers, and $s_{i_1}, ..., s_{i_n} \in S$.

For example, $s_1 s_2^3 s_1^{-5} s_2$ is a word in s_1, s_2 and their inverses.

The set S generates G if every element of G is expressible as a word in the elements of S and their inverses.

Fix a group G and a set S of generators $s_1, ..., s_n$ for G. For an element $w \in G$, choose an expression of w in terms of the s_i's that is as possible $w = s_{i_1}^{k_1} s_{i_2}^{k_2} ... s_{i_n}^{k_n}$, that is, we choose such an expression with minimal $|k_1|+|k_2|+...+|k_n|$. Then the length of w (with respect to S) is $l(w) = |k_1|+|k_2|+...+|k_n|$.

Public key cryptography (or asymmetric cryptography) has been the most significant and striking development in the history of cryptography. This revolutionary concept has been introduced in the famous paper "New Directions in Cryptography" [3]. Public Key cryptography, was invented by Diffie And Hellman more than forty years ago. In Public Key

cryptography, a user U has a pair of related keys (pK, sK): the key pK is public and should be available to everyone, while the key sK must be kept secret by U. The fact that sK is kept secret by a single entity creates an asymmetry, hence the name asymmetric cryptography.

III. Results

In the following proposition we present the public-key cryptosystem based on the word problem in a group.

Proposition 1:

Public-Key (pK)**:** a group G and two lists $S_A = \{a_1, ..., a_m\}$, $S_B = \{b_1, ..., b_n\}$ of elements of G.

Alice : choose a secret word $a = k_{pr,A}$ in S_A where $a = k_{pr,A} = a_1^{\epsilon_1} ... a_m^{\epsilon_m}$, for all $1 \leq i \leq m, a_i \in S_A$, $\epsilon_i = 1$ or $\epsilon_i = -1$.

Alice transmits to **Bob** the list $\left\{ab_1a^{-1}, ..., ab_na^{-1}\right\}$.

Bob: choose a secret word $b = k_{pr,B}$ in S_B where $b = k_{pr,B} = b_1^{\mu_1} ... b_n^{\mu_n}$, for all $1 \leq i \leq n, b_i \in S_B$, $\mu_i = 1$ or $\mu_i = -1$.

Bob transmits to **Alice** the list $\left\{ba_1b^{-1}, ..., ba_mb^{-1}\right\}$.

Encryption: to encrypt $m \in G$, **Alice** compute $c = a\left(ba_mb^{-1}\right)^{-\epsilon_m}\left(ba_{m-1}b^{-1}\right)^{-\epsilon_{m-1}} ... \left(ba_1b^{-1}\right)^{-\epsilon_1} m$.

Decryption: upon receipt c, **Bob** compute $b\left(ab_na^{-1}\right)^{-\mu_n}\left(ab_{n-1}a^{-1}\right)^{-\mu_{n-1}} ... \left(ab_1a^{-1}\right)^{-\mu_1} c = m$.

Proof:

Let $2 \leq i \leq m-1$, we compute $\left(ba_{i+1}b^{-1}\right)^{-\epsilon_{i+1}}\left(ba_ib^{-1}\right)^{-\epsilon_i}$, there is only four cases to be considered.

- If $\epsilon_{i+1} = 1, \epsilon_i = 1$, then $\left(ba_{i+1}b^{-1}\right)^{-\epsilon_{i+1}}\left(ba_ib^{-1}\right)^{-\epsilon_i}$ $= \left(ba_{i+1}b^{-1}\right)^{-1}\left(ba_ib^{-1}\right)^{-1} = ba_{i+1}^{-1}a_i^{-1}b^{-1}$.
- If $\epsilon_{i+1} = 1, \epsilon_i = -1$, then $\left(ba_{i+1}b^{-1}\right)^{-\epsilon_{i+1}}\left(ba_ib^{-1}\right)^{-\epsilon_i}$ $= \left(ba_{i+1}b^{-1}\right)^{-1}\left(ba_ib^{-1}\right)^{1} = ba_{i+1}^{-1}a_ib^{-1}$.
- If $\epsilon_{i+1} = -1, \epsilon_i = 1$, then $\left(ba_{i+1}b^{-1}\right)^{-\epsilon_{i+1}}\left(ba_ib^{-1}\right)^{-\epsilon_i}$ $= \left(ba_{i+1}b^{-1}\right)^{1}\left(ba_ib^{-1}\right)^{-1} = ba_{i+1}a_i^{-1}b^{-1}$.
- If $\epsilon_{i+1} = -1, \epsilon_i = -1$, then $\left(ba_{i+1}b^{-1}\right)^{-\epsilon_{i+1}}\left(ba_ib^{-1}\right)^{-\epsilon_i}$ $= \left(ba_{i+1}b^{-1}\right)^{1}\left(ba_ib^{-1}\right)^{1} = ba_{i+1}a_ib^{-1}$.

We have
$c = a\left(ba_mb^{-1}\right)^{-\epsilon_m}\left(ba_{m-1}b^{-1}\right)^{-\epsilon_{m-1}} ... \left(ba_1b^{-1}\right)^{-\epsilon_1} m$ $= \left(aba^{-1}b^{-1}\right) m$.

A similar argument shows that
Let $2 \leq i \leq n-1$, we compute $\left(ab_{i+1}a^{-1}\right)^{-\mu_{i+1}}\left(ab_ia^{-1}\right)^{-\mu_i}$, there is only four cases to be considered.

- If $\mu_{i+1} = 1, \mu_i = 1$, then $\left(ab_{i+1}a^{-1}\right)^{-\mu_{i+1}}\left(ab_ia^{-1}\right)^{-\mu_i}$ $= \left(ab_{i+1}a^{-1}\right)^{-1}\left(ab_ia^{-1}\right)^{-1} = ab_{i+1}^{-1}b_i^{-1}a^{-1}$.
- If $\mu_{i+1} = 1, \mu_i = -1$, then $\left(ab_{i+1}a^{-1}\right)^{-\mu_{i+1}}\left(ab_ia^{-1}\right)^{-\mu_i}$ $= \left(ab_{i+1}a^{-1}\right)^{-1}\left(ab_ia^{-1}\right)^{1} = ab_{i+1}^{-1}b_ia^{-1}$.
- If $\mu_{i+1} = -1, \mu_i = 1$, then $\left(ab_{i+1}a^{-1}\right)^{-\mu_{i+1}}\left(ab_ia^{-1}\right)^{-\mu_i}$ $= \left(ab_{i+1}a^{-1}\right)^{1}\left(ab_ia^{-1}\right)^{-1} = ab_{i+1}b_i^{-1}a^{-1}$.
- If $\mu_{i+1} = -1, \mu_i = -1$, then $\left(ab_{i+1}a^{-1}\right)^{-\mu_{i+1}}\left(ab_ia^{-1}\right)^{-\mu_i}$ $= \left(ab_{i+1}a^{-1}\right)^{1}\left(ab_ia^{-1}\right)^{1} = ab_{i+1}b_ia^{-1}$.

We have $b\left(ab_na^{-1}\right)^{-\mu_n}\left(ab_{n-1}a^{-1}\right)^{-\mu_{n-1}} ... \left(ab_1a^{-1}\right)^{-\mu_1} c$ $= bab^{-1}a^{-1}c = bab^{-1}a^{-1}\left(aba^{-1}b^{-1}\right) m = m$. ∎

Example 1:

Let $G = \left(\left\{1, x, x^2, y, xy, x^2y\right\}, \cdot\right)$ The Cayley table of $G = \left(\left\{1, x, x^2, y, xy, x^2y\right\}, \cdot\right)$ is defined as follows (see Table 1):

$\cdot$	1	x	x^2	y	xy	x^2y
1	1	x	x^2	y	xy	x^2y
x	x	x^2	1	xy	x^2y	y
x^2	x^2	1	x	x^2y	y	xy
y	y	x^2y	xy	1	x^2	x
xy	xy	y	x^2y	x	1	x^2
x^2y	x^2y	xy	y	x^2	x	1

Public-Key (pK)**:** a group $G = \left(\left\{1, x, x^2, y, xy, x^2y\right\}, \cdot\right)$ and two lists $S_A = \left\{x, x^2, y\right\}$, $S_B = \left\{xy, x^2y\right\}$ of elements of G.

Alice : choose a secret word $a = k_{pr,A}$ in S_A where $a = k_{pr,A} = x^{-1}x^2y^{-1} = x^2x^2y = xy$.

Alice transmits to **Bob** the list $\left\{(xy)(xy)(xy)^{-1}, (xy)\left(x^2y\right)(xy)^{-1}\right\} = \{xy, y\}$.

Bob : choose a secret word $b = k_{pr,B}$ in S_B where $b = k_{pr,B} = (xy)\left(x^2y\right)^{-1} = (xy)\left(x^2y\right) = x^2$.

Bob transmits to **Alice** the list $\left\{\left(x^2\right)(x)\left(x^2\right)^{-1}, \left(x^2\right)\left(x^2\right)\left(x^2\right)^{-1}, \left(x^2\right)(y)\left(x^2\right)^{-1}\right\}$ $= \left\{x, x^2, xy\right\}$.

Encryption: to encrypt $y \in G$, **Alice** compute $c = xy\,(xy)\left(x^2\right)^{-1}(x)\,y = x^2y$.

Decryption: upon receipt c **Bob** compute $x^2\,(y)\,(xy)^{-1}\,c = x^2\,(y)\,(xy)^{-1}\,x^2y = x^3y = y$.

IV. Conclusion

In this work, based on the hardness of the word problem in a group, we investigate the public key cryptosystem.

References

[1] B. Baumslag, B. Chandler, "Theory and Problems of Group Theory, Schaum's outline series, (1968).

[2] O. Bogopolski, Introduction to Group Theory", European Mathematical Society, (2008).

[3] W. Diffie, M. E. Hellman, "New Direction in Cryptography," IEEE Trans, on Inform Theory, 22(6), P. 644-665, (1976).

[4] D. Guin et T. Hausberger, "Algèbre Tome 1 Groupes, Corps et Théorie de Galois", EDP Sciences, (2008).

[5] J. Hoffstein, J. Pipher, J. H. Silverman, "An Introduction to Mathematical Cryptography, Springer, (2014).

[6] W. Ledermann, "Introduction to Group Theory, Longman, (1973).

[7] C. Paar, J. Pelzl, "Understanding Cryptography", Springer, (2010).

[8] L. Perret, "Etude d'Outils Algébriques et Combinatoires pour la Cryptographie à Clef Publique," thèse de doctorat, Universit´e de Marne–la–Vallée, (2005).

[9] H. Phan, P. Guillot," Preuves de Sécurité des Schémas Cryptographiques," université Paris 8, (2013).

[10] E. Post, "Recursive Unthenlvability of a Problem of Thue,", Journal of Symbolic Logic, 12(1):1-11, (1947).

[11] S. Qiao, W. Han, Y. Li and L. Jiao, "Construction of Extended Multivariante Public Key Cryptosystems," International Journal of Network Security, Vol. 18, No.1, pp. 60-67, (2016).

[12] N. R. Wagner, M. R. Magyarik. A Public Key Cryptosystem Based on the Word Problem. Proceedings of CRYPTO'84, LNCS 196, Springer-Verlag, pp. 19-36, (1985).

A New Approach to Verifying and Sharing a Secret QR Code using Elliptic Curves

Hichem BOUCHAKOUR ERRAHMANI
EEDIS - Djillali Liabes University
Sidi Bel Abbes, Algeria
Computer Science dept.
Belhadj Bouchaib Center-University
Ain Temouchent, Algeria
b_hichem@hotmail.fr

Hind IKNI
Computer Science dept.
Belhadj Bouchaib Center-University
Ain Temouchent, Algeria
hind.ikni@gmail.com

***Abstract*—One of the modern applications of cryptography is the sharing of secrets in occurrence keys. Indeed, the need to establish a shared secret key in a multi-user system clearly remains a major problem of trust between users. Therefore, one solution is to share this secret key between users seamlessly. New technologies embedded systems such as sensor networks provide an ideal platform for sharing secrets. In addition, elliptic curves offer an adequate solution for reducing the size of keys, which is suitable for embedded systems. In this article, we propose an approach for sharing a secret leaked in a QR code adapted for a multiuser system, where each user has the ability to verify its share by an access structure. The system allows a recovery without loss of data in this case the QR code used.**

Keywords— Elliptic Curve Cryptography, Discrete Logarithm Problem, Image Secret Sharing, Verifiable Secret Sharing.

I. INTRODUCTION

Classical cryptography treats the notions of encryption, decryption, hashing ... using secret keys whose owners are the actors of the cryptosystem. Those keys represent the security basis of the entire system according to Kerckhoffs principles. On the other hand, the question that could arises in our mind, is how to protect such an important key? Hence, the notion of threshold secret sharing, where the key is distributed over a group of participants in such a way that none of them possesses an information about the secret, but some candidates representing the access structure collaborate at its reconstitution. Several works have contributed to improve secret sharing since the first approach of Adi Shamir, such as verifiable approaches and proactive ones. However, the particularity of contemporary methods lies in the use of elliptic curves, for the reason that they revolutionized cryptosystems security by providing solutions to constraints caused by key size and operations complexity. In this paper, we propose a method of securing visual cryptographic keys by multi secrets sharing scheme with self-selecting of private ones, based on ECDLP. The scheme takes as input an image matrix which represents the secret to share on a server–client network without information loss. In our method, we give the participants the capability to verify their received shares without secret reconstruction, to prove the validity of the dealer, shadows, and even candidates. The rest of the paper is structured as follows: Section II illustrates preliminaries techniques for a good comprehension of the subject. Section III presents related works for sharing secrets using elliptic curves. Section VI describes steps of the proposed approach. Section V discuses results. Finally, section IV concludes and resumes the paper.

II. PRELIMINARIES

In this section, we describe briefly the basic techniques used for secret sharing with elliptic curves.

A. Elliptic Curve

An elliptic curve Eover a finite field $\mathbb{F}_p$ is a set of pairs $(X, Y) \in \mathbb{F}_p^2$ resolving the equation $Y^2 = X^3 + A \cdot X + B\ (modp)$ union a particular element called point at infinity noted $\mathcal{O}$ (with $A, B \in \mathbb{F}_p$ and $4A^3 + 27B^2 \neq 0\ (modp)$). We should mention some operations properties over $E(\mathbb{F}_p)$[1]:

a) Closure: $\forall P, Q \in E$, if$P + Q = R$then$R \in E$;

b) Associativity: $\forall P, Q, R \in E, (P + Q) + R = P + (Q + R)$;

c) Identity element: $\forall P \in E, P + \mathcal{O} = \mathcal{O} + P = P$;

d) Inverse element: $\forall P(x, y) \in E, \exists -P(x, -y) \in E$;

e) Commutativity: $\forall P, Q \in E: P + Q = Q + P$;

We infer that $E(\mathbb{F}_p)$ forms an abelian group.

The addition operation in $E(\mathbb{F}_p)$ is defined as follows:

For each $P(x_P, y_P), Q(x_Q, y_Q), R(x_R, y_R) \in E$ and $P + Q = R$

$$x_R = \gamma^2 - x_P - x_Q\ (mod\ p)$$

$$\text{And } y_R = \gamma(x_P - x_R) - y_P\ (mod\ p)$$

Such that:

$$\gamma = \begin{cases} (y_Q - y_P)(x_Q - x_P)^{-1} (\text{mod p}) & if\ P \neq Q \\ (3x_P^2 + A)(2y_P)^{-1} (\text{mod p}) & else \end{cases}$$

The inverse of R is obtained by $-y_R\ (mod\ p)$.

Given a large prime number p, finding the integer n such that $Q = n \cdot P$ where $P, Q \in E(\mathbb{F}_p)$, is a very hard problem to solve. This problem is called the Elliptic Curve Discrete Logarithm Problem (ECDLP), which makes a good tool for cryptographer.

B. Threshold secret sharing of Shamir

A threshold secret sharing scheme consists to split a secret key and distribute it among $n$participants in such a way its reconstitution requires only a qualified group of them.

In its paper, Shamir [1] describes the conditions of a threshold (k, n) sharing system:

- knowledge of any k or more pieces of the secret, makes it easily computable;

- Knowledge of any $k-1$ or fewer pieces of the secret leaves it completely undetermined.

To share a secret S among n persons with a threshold k, we define a random $k-1$ polynomial

$$f(x) = a_0 + a_1 x + \cdots + a_{k-1} x^{k-1}$$

in which $a_0 = S$ and $a_1, \cdots, a_{k-1} \in \mathbb{R}$. To determine the different shares, we compute n points $(i, f(i))$.

For secret reconstruction, we use Lagrange interpolation for k given points:

$$P_n(x) = \sum_{i=0}^{n} y_i \prod_{\substack{k=1 \\ k \neq i}}^{k=n} \frac{(x - x_k)}{(x_i - x_k)}$$

III. Related Works

The first threshold secret sharing scheme was invented in 1979; we owe it to A.Shamir [2]. Also called (t, n) scheme, his approach is based on Lagrange Polynomial Interpolation, where a secret can be distributed over n participants, and reconstructed by at least t of them.

In the same year, a geometric approach was published by G.Blakley [3], who represented the secret by an intersection point of hyper plans, in such a way that each candidate receives one hyper plan equation.

Several techniques of sharing secret have followed, adding some options to main ideas. A notion of sharing multi secrets was treated in different approaches. Based on Shamir's scheme and Elliptic Curve, Hua Sun [4] and Binu [5] have both published a method where a set of secrets are shared by Shamir's polynomial coefficients using elliptic curves bilinear pairing and a cryptographic hash function.

Moreover, to study key management for MANETs, H. Dahshan[6]put forward a new scheme for sharing a matrix of secrets among mobile nodes using Lagrange Polynomial Interpolation and ECDLP. His method is divided in two main parts, an offline initialization phase where a central authority distributes pairs of long term public/private keys for each node, and an online phase in which the node with the largest identity number considered as a dealer, generates session keys using his own long term private key, then collects public session keys to reconstruct secrets by interpolation.

Furthermore, Chaitanya [7] proposed a scheme for MANETs based on Shamir's approach; however, he adopted it with bivariate polynomial which allows scalability of his system.

For another type of networks system, Al-Adhami [8] designed a threshold quorum system allowing a secure distribution of logistics information on RFID Tags, where the shares are stored encrypted using El Gamal ECC scheme, which provides security and privacy during package transmission. Thus, according to the authors, the quorum system maintains information security against several RFID attacks.

In order to have more efficiency, a verification option technique was proposed. In 1991, Pedersen [9] build a signed threshold sharing scheme assigning to each candidate additional information allowing him to verify the validity of his own share using Discrete Logarithm Problem (DLP).

After that, H.Yiliang [10] constructed a sharing cryptosystem based on Pedersen's theory using Elliptic Curve Signature Algorithm (ECSA) and Elliptic Curve Encryption System (ECES) based on ECDLP, the author claims that the scheme resists to attacks but requires safe transmission channels.

In the other hand, Patel [11] have propounded a different verifiable multi secrets sharing scheme where he overcomes channels security weaknesses by using Double Knapsack algorithm to secure transmissions.

In another side, different schemes are built with self-selecting secret key option based on ECDLP, where each participant chooses a private key by himself for the sharing operation. W.Caimei's[12] scheme uses Diffie-Hellman elliptic key exchange algorithm to generate the private key point coordinate and exploits a cryptographic hashing function to secure them.

IV. Scheme Description

Our proposed scheme treats a secrets sharing method on a distributed system, where secrets are represented by each pixel of a given image. Two servers are used for the network communication as shown in Fig. 1, one as a Dealer for sharing parameters initialization system, publishing them and distributing the shares. The second server, called Combiner, is used only for secrets reconstruction

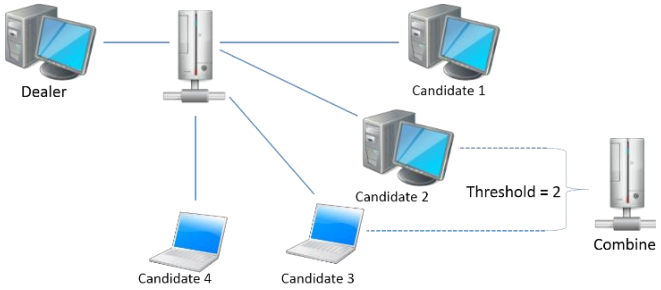


Fig. 1. Network architecture

computation where the threshold participants collaborate by connecting to it.

A. Sharing system initialization

All mathematic notations used in the scheme are shown in TABLE. I. It's the role of the Dealer to initialize the settings for the sharing system. Since all cryptographic arithmetic operations require an elliptic curve over a finite field, the Dealer chooses first a big prime p and an appropriate cryptographic elliptic curve

$$E(\mathbb{F}_p): y^2 = x^3 + ax + b \ (mod\ p)$$

Where $a, b \in \mathbb{F}_p$, he selects a base point generator $G(x_G, y_G)$ such that $\#E \cdot G = \mathcal{O}$.

Besides, an image of size $T = L \times C$ is required to represent the matrix of secrets M, where each pixel is considered as a unique secret to share. Finally, the Dealer publishes the parameters $< p, E, G, L, C >$.

B. Shares distribution

In the proposed scheme, each candidate u_i is identified by a unique number *nonce* which is generated once a client connected to the server. u_i generates his own private sharing keys in matrix form, using published parameters, where each element s^i is randomly chosen over $\mathbb{F}_p$

$$S^i = \begin{pmatrix} s_{11}^i & \cdots & s_{1C}^i \\ \vdots & \ddots & \vdots \\ s_{L1}^i & \cdots & s_{LC}^i \end{pmatrix} \quad (1)$$

TABLE. I. MATHEMATICAL NOTATIONS

Symbol	Description
p	Prime number
$\mathbb{F}_p$	Finite field
E	Elliptic curve $y^2 = x^3 + ax + b\ (mod\ p)$
O	Point at infinity
$\#E$	Number points
G	Base point
U	Set of all participants
$u_i \in U$	A unique participant
$n = \lvert U \rvert$	Number of participants
k	Threshold
T	Size of the secret matrix
M	The secret matrix
s^i	Private key of participant u_i
L	Lines of a matrix
C	Columns of a matrix

then calculates his public keys by ECDLP using G to generate T public points P_{lc}^i:

$$S^i \cdot G = \begin{pmatrix} s_{11}^i \cdot G & \cdots & s_{1C}^i \cdot G \\ \vdots & \ddots & \vdots \\ s_{L1}^i \cdot G & \cdots & s_{LC}^i \cdot G \end{pmatrix} = P^i = \begin{pmatrix} P_{11}^i & \cdots & P_{1C}^i \\ \vdots & \ddots & \vdots \\ P_{L1}^i & \cdots & P_{LC}^i \end{pmatrix} \quad (2)$$

After collecting all public key matrices P^i, the Dealer prepare the shares in several steps :

- **Step 1**He verifies the distinction of all public keys collected from each other's. For each $P^i = P^j$ he replies to u_i andu_j asking for other matrices, where the specific candidates generate an other private keys matrix S^i to compute different public matrix P^i. The Dealer iterates this procedure until collecting n different matrices.
- **Step 2** He chooses his private key $r \in \mathbb{F}_p$ to generate a private matrix of points Q^i:

$$r \cdot P^i = \begin{pmatrix} r \cdot P_{11}^i & \cdots & r \cdot P_{1C}^i \\ \vdots & \ddots & \vdots \\ r \cdot P_{L1}^i & \cdots & r \cdot P_{LC}^i \end{pmatrix} = Q^i = \begin{pmatrix} Q_{11}^i & \cdots & Q_{1C}^i \\ \vdots & \ddots & \vdots \\ Q_{L1}^i & \cdots & Q_{LC}^i \end{pmatrix} \quad (3)$$

Where each point Q_{lc}^i has coordinates (X_{lc}^i, Y_{lc}^i).

- **Step 3** The secret matrix M is obtained by converting a given image pixels to elements over $\mathbb{F}_p$:

$$M = \begin{pmatrix} M_{11} & \cdots & M_{1C} \\ \vdots & \ddots & \vdots \\ M_{L1} & \cdots & M_{LC} \end{pmatrix} \quad (4)$$

- **Step 4** For each secret element M_{lc} of the matrix, the Dealer randomly generates a k degree polynomial according to Shamir's scheme:

$$f_{lc}\ (x) = \sum_{i=0}^{k-1} a_{i,lc} \cdot X^i\ (mod\ p) \quad (5)$$

Where $a_{0,lc} = M_{lc}$ and $a_{i,lc}$ with $1 \leq i \leq -1$ randomly chosen over $\mathbb{F}_p$ to obtain a matrix of polynomials :

$$F = \begin{pmatrix} f_{11} & \cdots & f_{1C} \\ \vdots & \ddots & \vdots \\ f_{L1} & \cdots & f_{LC} \end{pmatrix} \quad (6)$$

- **Step 5** To compute the shares of each participant, the Dealer determines the polynomial image of each X_{lc}^i coordinate of Q_{lc}^i by the adequate polynomial f_{lc}, to

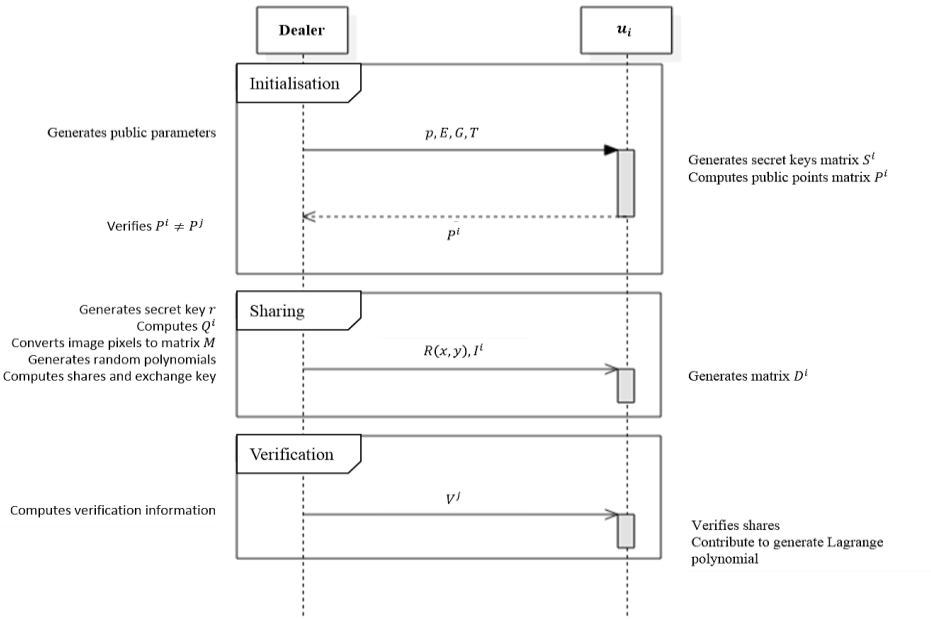


Fig. 2. Approach sequence diagram

generate n shares matrices I^i also called shadows:

$$I^i = \begin{pmatrix} f_{11}(X_{11}^i) & \cdots & f_{1C}(X_{1C}^i) \\ \vdots & \ddots & \vdots \\ f_{L1}(X_{L1}^i) & \cdots & f_{LC}(X_{LC}^i) \end{pmatrix} = \begin{pmatrix} I_{11}^i & \cdots & I_{1C}^i \\ \vdots & \ddots & \vdots \\ I_{L1}^i & \cdots & I_{LC}^i \end{pmatrix} \quad (7)$$

- **Step 6** Finally, the Dealer publishes a public key point R generated by ECDLP to exchange private points matrix:

$$R = r \cdot G \ (mod\ p) \quad (8)$$

C. Secrets reconstitution

For secrets reconstruction, k participants u_j are required to collaborate in order to construct Lagrange polynomial using I^i matrices and the public point R.

- **Step 1** At first, each candidate u_j computes the matrix of points for interpolation using private keys matrix S^j.

$$D^j = S^j \cdot R = \begin{pmatrix} D_{11}^j & \cdots & D_{1C}^j \\ \vdots & \ddots & \vdots \\ D_{L1}^j & \cdots & D_{LC}^j \end{pmatrix} \quad (9)$$

- **Step 2** the Combiner construct a Lagrange polynomial for each secret of the matrix M using D_{lc}^j abscissa.

$$P_n(x) = \sum_{i=1}^{k} I_{lc}^i \prod_{\substack{j=1 \\ j \neq i}}^{k} \frac{(x - X_{lc}^j)}{(X_{lc}^i - X_{lc}^j)} \quad (10)$$

D. Non interactive verification of shares

In our approach, each candidate has independently the capability to verify the validity of his shadow at any time, even without collaborating to reconstruct the main secret matrix, using additional information computed by the Dealer and broadcasted to all participants.

According to every polynomial coefficient a_j for each secret element M_{lc} with $0 \leq j \leq k-1$, the Dealer computes with ECDLP k pointsv_{lc}^j:

$$v_{lc}^j = a_{lc}^j \cdot G \ (mod\ p) \quad (11)$$

Then regroups all v_{lc}^j points corresponding to each secret in a matrix V^j, k matrices will be broadcasted :

$$V^j = \begin{pmatrix} v_{11}^i & \cdots & v_{1C}^i \\ \vdots & \ddots & \vdots \\ v_{L1}^i & \cdots & v_{LC}^i \end{pmatrix} \quad (12)$$

So, each candidate will be able to check the validity of his matrix shares by the formula:

$$I_{lc}^i \cdot G = \sum_{j=0}^{k-1} (X_{lc}^i)^j \cdot v_{lc}^j \ (mod\ p) \quad (13)$$

If it returns true, the share is correct and can fit for the recovery formula. If not, the participant publishes a notification warning.

E. Correctness

In this subsection, we give the proofs to the correctness of key exchange equation for the sharing operation and the verification formula.

1) Key exchange proof : Candidate u_j computes at the beginning the public point P using his private key S by ECDLP (2) that he sends to the Dealer publically, this last at his turn computes the private points Q also by ECDLP using his own private key r (3), which coordinates have been exploited in Shamir's polynomial (7).

$$Q_{lc}^j = r \cdot P_{lc}^j = r \cdot s_{lc}^j \cdot G = s_{lc}^j \cdot R = D_{lc}^j \quad (14)$$

so, $k$participant u_j can recover the secrets using matrices D^j (10) coordinates.

2) Verification proof : Any participant u_i can verify the intercepted share by ECDLP according to the formula :

$$\begin{aligned} I_{lc}^i \cdot G &= f_{lc}(X_{lc}^i) \cdot G \ (mod\ p) \\ &= \left(\sum_{j=0}^{k-1} a_{j,lc} \cdot (X_{lc}^i)^j \ (mod\ p) \right) \cdot G \\ &= \sum_{j=0}^{k-1} a_{j,lc} \cdot G \cdot (X_{lc}^i)^j \ (mod\ p) \\ &= \sum_{j=0}^{k-1} v_{lc}^j \cdot (X_{lc}^i)^j \ (mod\ p) \end{aligned} \quad (15)$$

V. Results and Discussion

In this section, we demonstrate the feasibility of the proposed method by exposing experimental results in timing, non-loss information after recovery and security efficiency.

A. Non-loss information

To prove the scheme efficiency with non-loss information, we tested it on a QR digital image of 33×33 px Fig. 3, which gives after conversion a secret matrix of big values with the same size, each pixel (element of the matrix) is represented in the same bit length as the curve field chosen.

To ensure that the shadow does not reveal any information about the original secret, we present the greyscale histogram of both, the main image secret and the shadows Fig. 4 were we can observe the distinction of frequencies for the same ranges. Results are obtained from a sharing with a threshold equal to 3 using a cryptographic elliptic curve over 192 bits prime field (NIST P-192).

To prove the scheme validity, we use a QR code reader to extract the secret from the reconstructed image so we get the original plain text hidden inside.

B. Timing results

TABLE. II represents the different timing measures computed during 4 tests to evaluate the performance of our application, incrementing each time the threshold value. From these results, we conclude that keys calculation and verification operations are computationally more expensive than Shamir's sharing and Lagrange interpolation algorithm, this is due to the complicated process of ECDLP with a large prime (192 bits) and for a matrix of 33×33 of big bit length values.

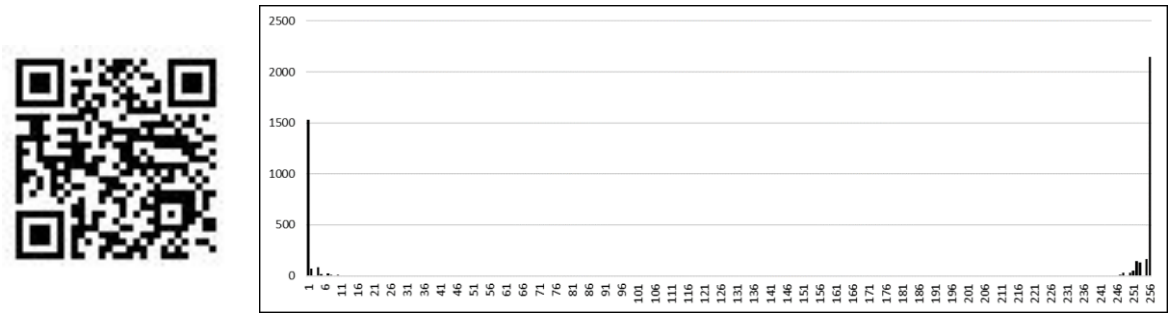


Fig. 3. Original secret image shared and its histogram

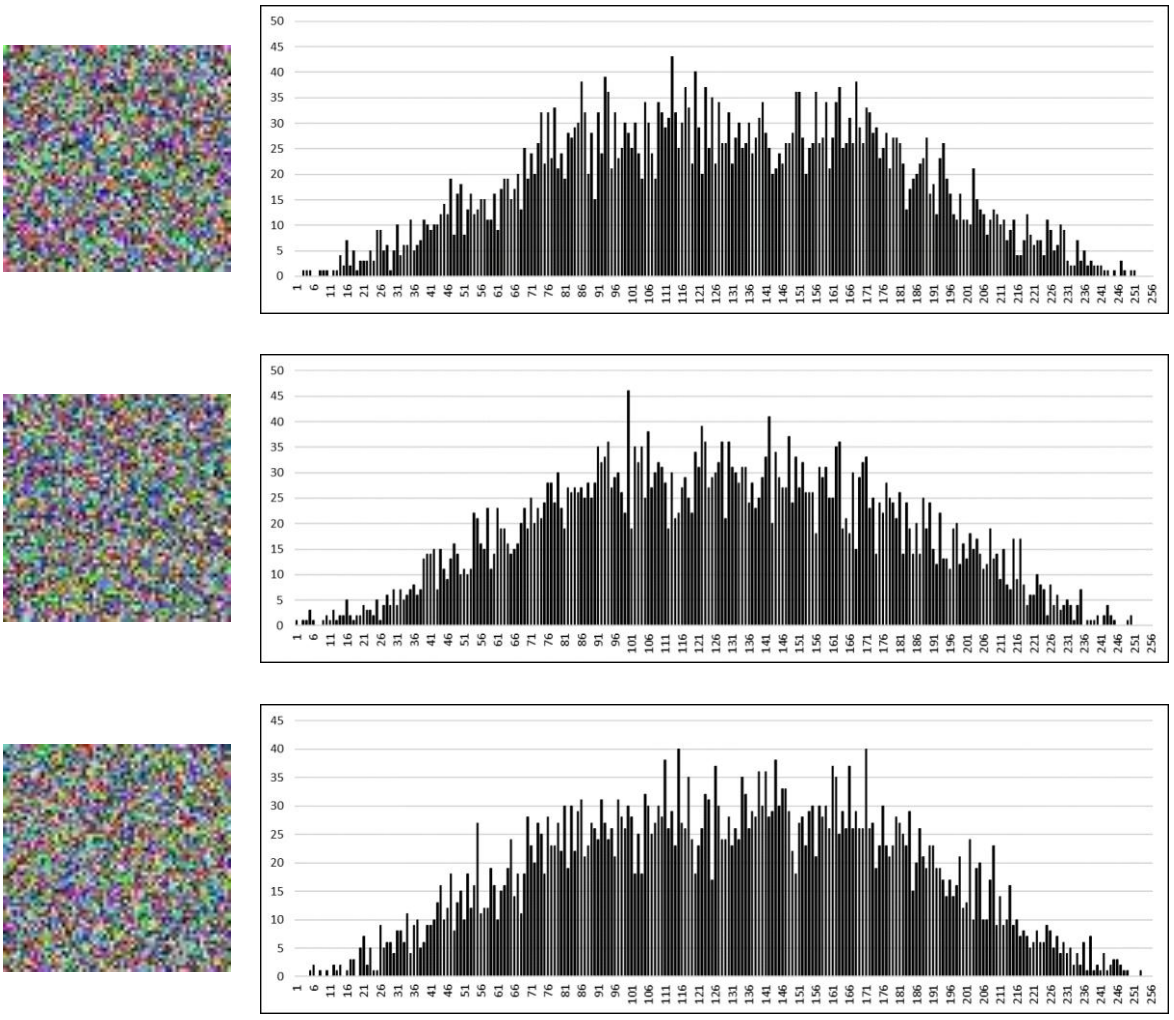


Fig. 4. Shares (shadows) obtained and their histogram

TABLE. II. PROPOSED SCHEME TIMING RESULTS IN MS FOR 33×33 MATRIX

Threshold	**Average computations**				**Reconstitution**
	Generation verification information V	***Points matrices ECDLP***	***Shamir's sharing***	***Verification***	
2	8037	7022	4	19835	184
3	14514	7027	**13**	39775	312
4	21619	6923	15	65343	431
5	28266	7037	18	99543	635

TABLE. III. PERFORMANCE AND SECURITY COMPARISON

Scheme	Secure initial distribution keys	Secure combining channel	Share security	Malicious shares detection	Recovery type
Proposed	On line and Not required (self-selecting sharing key)	Required	Secured (Meaningless)	Yes	Lossless
Ref [6]	Off line	Required	Secured (Refreshed))	Yes	Lossless
Ref [7]	Not mentioned	Not mentioned	Secured (Refreshed)	Yes	Lossless
Ref [8]	On line and Not required	Required	Secured (Encrypted)	Yes	Lossless
Ref [11]	On line and Not required (self-selecting sharing key)	Public (Double Knapsack)	Secured	Yes	Lossless

C. Security efficiency

From the shadows histogram, we conclude that the scheme is not sensitive to the threshold value, whether shares are generated with $k = 2$ or $k = 5$, we still obtain histograms with no information about the original image.

Before talking about security aspect, we must elucidate an important notion about the proposed architecture. Communications with the Dealer does not require a high security channel, he is considered as the unique distant person possessing the secret, and all parameters sent or received by him are either public, broadcasted or transferred no plain information. On the other hand, contribution to reconstruct the secret requires a server combiner in a local network with high security channels.

In a secret sharing system, we have two categories of attacks, from outside or inside the system. For insider attacks, the scheme allows each candidate to verify the integrity of his shadow, even the combiner is in ability to verify shares of each one of them, which revealed any malicious information in the system. Intercepting the whole shadows requires an attacker knowing the exact timing of shares transmission, because participants are independent and there is no interaction between them. Hence, an intruder cannot reconstruct the secret even if he intercepts some shadows because he does not possess the secret keys.

D. Comparison

The proposed approach is compared in TABLE. III with some typical existing works in term of performance and security. Moreover, in TABLE. IV we present a comparison with Dahshan's[4] scheme in term of verification timing, since the structure of secrets in both works are similar. For e.g. the results of this test on an image size matrix 24×16px with a threshold of 5 participantsand elliptic curve field of 192bits length are as follows; ECDLP matrix points computations are measured to an average of 2615ms, while the shadows matrix calculations run into just 4ms and for the recovery operation takes 385ms. For the verification we measure the timing of the matrices generation by the Dealer which runs in 10113ms, and the verifying operation by the candidates, whose average is equal to 35526ms, which is 2000ms less than Dahshan's scheme value for the same parameters.

VI. CONCLUSION

In this paper, we proposed a verifiable image self-selecting secret sharing scheme for any server-client network like distributed systems, based on Shamir's secret sharing and ECDLP. The method takes as main parameters an image that represents our secret and an elliptic curve over a prime finite field. A threshold must also be specified, in order to recover the secret. The method allows also verification of shares validity. The non-loss information is proved by QR secret recovery and gray scale histogram shadows ensure the security efficiency of the sharing. Timing measures demonstrates the complexity of ECDLP algorithm. The results have been proved in comparison section. As a perspective, we propose to develop the scheme with more options like shares refreshing in order to decrease the time validity of each shadow.

TABLE. IV. VERIFICATION TIMING COMPARISON IN MS

scheme	Matrix	Curve	Threshold	Verification
Dahshan scheme	24×16	192 bits	5	37380
		256 bits		67912
Proposed scheme	24×16	192 bits	5	35526
		256 bits		64271

REFERENCES

[1] Bouchakour Errahmani, H., & Faraoun, K. (2018). Towards a Hybrid Approach Based on Elliptic Curves and Cellular Automata to Encrypt Images. *Journal of Information Security Research*.

[2] Shamir,A. (1979). How to share a secret. *Communications of the ACM*, 612-613.

[3] Blakley, G. R. (1979). Safeguarding cryptographic keys. *Proceedings of the national computer conference*, pp. 313-317.

[4] Hua, S. a. (2010). A multi-secret sharing scheme with general access structures based on elliptic curve. *Advanced computer theory and engineering (ICACTE), 2010 3rd international conference, IEEE*.

[5] Binu, V., & Sreekumar, A. (2017). Secure and Efficient Secret Sharing Scheme with General Access Structures Based on Elliptic Curve and Pairing. Wireless Personal Communications, 1531--1543.

[6] Dahshan, H. a. (2011). An elliptic curve secret sharing key management scheme for mobile ad hoc networks. Security and Communication Networks, 1405-1419.

[7] Kumar, C., Basit, A., Singh, P., & Venkaiah, V. C. (2017). Proactive secret sharing for long lived MANETs using Elliptic Curve Cryptography. *International Conference on Inventive Computing and Informatics*. Coimbatore, Chennai: ResearchGate.

[8] Al-Adhami, A., Ambroze, M., Stengel, I., & Tomlinson, M. (2016). A Quorum System for Distributing RFID Tags. *Intl IEEE Conferences on Ubiquitous Intelligence & Computing, Advanced and Trusted Computing, Scalable Computing,* (pp. 510--517).

[9] Pedersen, T. P. (1991). Distributed provers with applications to undeniable signatures. *Workshop on the Theory and Application of of Cryptographic Techniques, Springer*, pp. 221-242.

[10] Han, Y. a. (2003). Verifiable threshold cryptosystems based on elliptic curve. Computer Networks and Mobile Computing, 2003. ICCNMC 2003. 2003 International Conference, IEEE, pp. 334-337.

[11] Nisha, P. D. (2016). A Novel Verifiable Multi-Secret Sharing Scheme Based on Elliptic Curve Cryptography. *The Tenth International Conference on Emerging Security Information, Systems and Technologies, IARIA*.

[12] Caimei, W. a. (2009). Self-selecting Sub-secret Keys Sharing Scheme Based on Polynomials over Elliptic Curve. *Information Assurance and Security, 2009. IAS'09. Fifth International Conference, IEEE*, pp. 734-737.

Security Enhancements of A5/1 Based Particle Swarm Optimization for Mobile Telecommunication Networks

Abdelkader GHAZLI[12], *Adda ALIPACHA*[1], *Naima HADJ SAID*[1], *Boubakeur Ghazli* [2]
Coding and Information Security Laboratory (LACOSI), ALGERIA [1]
Tahri Mohamed University of Bechar [2]
Ghazek@gmail.com

Abstract

In cellular networks the series of algorithms A5 are used to ensure the communications between the different subscribers of the network. A5/1 is the strong known encryption algorithm which protects the air interface of the mobile network. However, this algorithm sufferer for a lot off problems especially in the clocking mechanism which control the clocking of registers that composes the A5/1 stream cipher. For this raison, several attacks have been published aimed to cryptanalyzing this algorithm such as time memory trade off attacks, guess and determine attacks, biased birthday attack [1] and the random subgraph attack. [2]

This paper propose new security enhancements to improve A5/1 encryption algorithm based on new particle swarm optimization (PSO) control mechanism in order to make the A5/1 stream cipher robust and more resistive to some attacks and to be used in future mobile communication systems.

The improvements that make both attacks impractical do not change the architecture of the conventional A5/1 and aims to increase the complexity of the A5 algorithm by making its clocking mechanism more complex by the integration of a new function to be optimized by the PSO algorithm which it have been successfully used to solve a wide array of different optimization problems.

Keywords: A5/1, PSO, LFSR, Stream Cipher, Security, GSM, Mobile Network

INTRODUCTION

Today we see almost everyone has a cellular phone connected to the internet or some other networks. Our life is changed and new things have emerged such as M-commerce where monetary transactions are conducted via a mobile network.

Mobile communication use wireless connectivity to facilitate people communication anywhere and at any time. However, the openness of mobile communication poses several security threats and consequently the mobile operators use some techniques to ensure the security of subscriber communications including the encryption of information interchanged in the air interface between the mobile device and its network. The encryption in mobile phone communications is achieved by using stream ciphers which are symmetric key ciphers that generate pseudorandom binary patterns which are used to encrypt the message signals on bit-by-bit basis. Stream ciphers are much faster than block ciphers and usually need fewer resources for implementation in hardware and software. For these raisons, stream ciphers are more suitable for telecommunication applications such as mobile phone networks.

Information security over mobile communication networks is vital and presents a crucial issue for the security of mobile communications. To provide privacy on air communication, voice calls in mobile phone communications are encrypted using a family of algorithms called A5.

A5/1 is the stronger version and A5/2 is the weaker one while the A5/3 which is used in 3G is a block cipher. The algorithm A5/1 consists essentially of three linear feedback shift registers LFSR controlled by a clocking mechanism which is based on a majority function to make a decision whether a register is shifted or not. Due to the security limitation in the architecture of A5/1 It is susceptible to several attacks and most of these attacks against A5/1 stream cipher use the security failing in its clocking mechanism. [3] Consequently, a lot off attacks against A5/1 was been published.

Particle Swarm Optimization (PSO) is a family of algorithms which can be used to find near or optimal solutions to some problems. It is easily implemented and has proven both very effective and quick when applied to a various set of optimization problems.

Several approaches have been proposed in the literature to improve the shift control mechanism of the various linear feedback shift registers R1, R2 and R3 which constructs the conventional A5/1. Many of these approaches define new mechanisms that attempt to construct a pseudo-random generator that produces binary sequences of good random characteristics but without using any decisive factor that assured the convergence of the algorithm to a desired solution. The present approach makes the problem of shifting of registers as a problem of optimization using the particle swarm optimization algorithm. In our proposed approach, the shift of any register is performed by satisfying a certain function which serves to maximize the random character quality produced by our generator called A5/PSO.

A new technique is also used to shift linear feedback shift registersR1, R2 and R3 that build the conventional A5/1 which is shifting any register using a certain speed which designates the number of times a register is shifted in a clock top. This new functionality attempts to load the register in question rapidly by new values so that the generator can produce binary sequences of good randomness.

SECURITY IN MOBILE TELECOMMUNICATION NETWORKS

Many cryptosystem are used in mobile telecommunication networks to satisfy the requirements of confidentiality and integrity of communications and to authenticate mobile terminals. The use of this or that cryptosystem is essentially depends on the intended security function and the network generation considered. GSM (2G), GPRS (2.5G), EDGE (2.75G), UMTS (3G) and LTE (4G).

The authentication protocol used in GSM networks is based on a symmetric cryptosystem called A3. The authentication of a mobile device consists of calculating a signed response, designated SRES of 64 bits, requires a 128-bit symmetrical Ki key and a 128-bit RAND challenge sent by the operator. The calculation of SRES is carried out jointly by the smart card of the mobile and by the authentication center of the operator. Authentication is accepted in case of equality of values of SRES calculated by the authentication center of the operator and that sent by the mobile device.

A key derivation algorithm called A8 is used to produce a symmetric key Kc of 64 bits from Ki and RAND. This session key Kc serves to encrypt the communications; it is generated by the terminal's smart card and by the Authentication center on the other hand. The smart card provides Kc to the mobile terminal for encrypting mobile communication.

Cryptographic algorithms are implemented to protect the confidentiality of data exchanged through radio frequency communications. Encryption covers all traffic and signaling. There is in fact a series of cryptographic algorithms grouped under the name A5 including A5/1, A5/2 and A5/3. The choice of the algorithm to be used for a communication is negotiated, the network choosing an algorithm from the list of those proposed by the terminal. This list contains at least A5/1.

A GSM conversation is performed by division into time blocks, each of which lasts 4.6 milliseconds and contains 2 × 114 bits for both communication channels. A session key Kc is used with a block counters Fn to constitute the initial state of a pseudorandom number generator that produces 228 bits. These are used for encryption after an XOR with data from both channels.

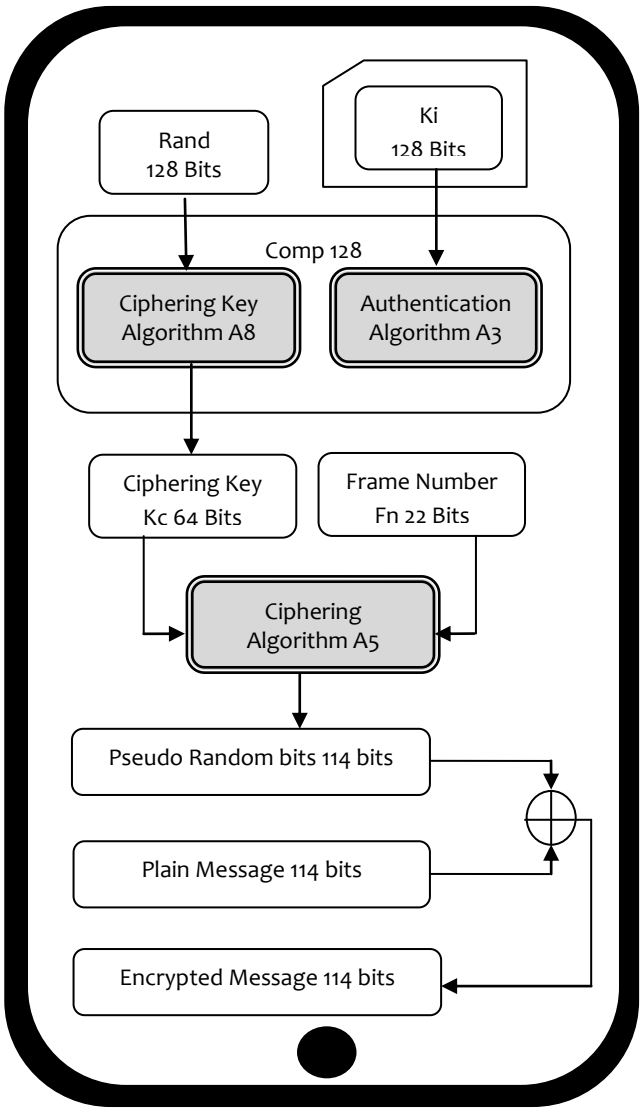


Figure 1: GSM Security Algorithms

Description of A5/1 stream cipher

A5/1 is a stream cipher used to provide over-the-air communication privacy in the GSM cellular telephone standard. It is used in Europe and the United States. In GSM networks, transmission is drive as a sequence of frames called sent every 4.615 milliseconds. The frame length is 228 bits, 114 bits for the communication in each direction. A5/1 is used to produce for each frame a 228 bit sequence of key stream which is XORed with the 228 bits of the frame.

A5/1 is built from three short linear feedback shift registers LFSR of lengths 19,22, a nd 23 bits denoted by R1, R2 and R3 respectively. A5/1 is initialized using a 64 bit key generated to drive each conversation called Kc and frame counter Fn of 22 bit which is publicly known. The taps of R1 are at bit positions 13, 16, 17 and 18. the taps of R2 are at bit positions 20,21 and the taps of R3 are at bit positions 7, 20,2 1,22.

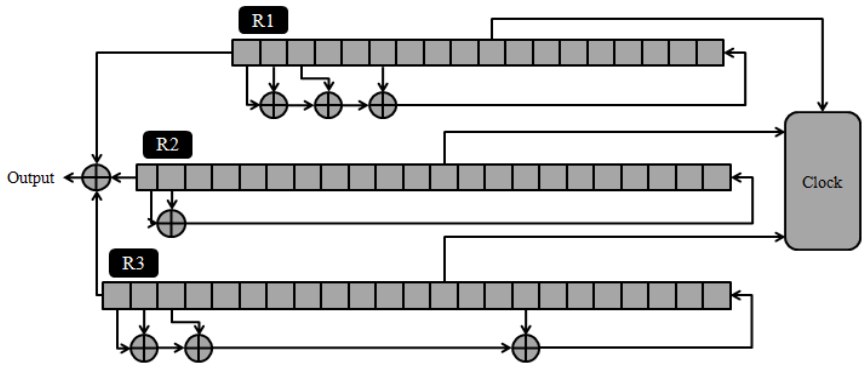


Figure 2: A5/1 Stream Cipher

The algorithm A5 is unfolded in four steps:

Step 1: Reset: all registers R1, R2 and R3 are initialized to zero.

Step 2: Initialization: Load 64 bits of the ciphering key Kc and 22 bits of frame number Fn into all of the three registers by xoring each bit of Kc and Fn with the least significant bits of each register, registers clocked regularly.

Step 3: Warm-up: Clock for 100 cycles and discard the output, registers clocked irregularly.

Step 4: Execution: Clock for 228 cycles, generate 114+114 bits, registers clocked irregularly.

Particle Swarm Optimization

Optimization determines the best suited solution to a problem under given condition. Swarm intelligence (SI) is based on the collective behavior of decentralized, self organized systems. It may be natural or artificial. Natural examples of SI are ant colonies, fish schooling, bird flocking, and bee swarming. PSO (Particle Swarm Optimization) is a computation technique population based optimization method like genetic algorithms. It was developed in 1995 by Kennedy and Eberhart. This technique was successfully used to solve some optimization problems of such as neural network training, functions optimization, fuzzy control and also in classification problems.

The PSO is initialized with a population of m random solutions of the fitness function. Each individual solution pi , i = 1, 2, ..., m, in the swarm is considered as a particle. Essentially PSO algorithm is identified by two parameters velocity and position. In each iteration, the velocity Vi and the position Xi of each particle are updated according to the fitness values of the updated individuals, the personal best position pBest of each particle and the global best position gBest among all the particles are updated.[4]

Each particle pk is influenced by its personal best position pBest and the global best position gBest . Therefore, the PSO searches the global optimum solution by adjusting the trajectory of each particle toward its personal best position and the global best position.

$V_i = w * V_i + c_1 * r_1 * (pBest_i - X_i) + c_2 * r_2 * (gBest - X_i)$
$V_i = X_i + V_i$ where:

Xi: The current position of the particle, Vi: The current velocity of the particle, i =1,2,… ..,m
PBesti: The personal best position of the particle, gBest: The global best position of all the particles.

w: is the inertia which is used to control the impact of previous velocities value. A larger inertia weight ω facilitates global exploration (searching new areas) while a smaller inertia weight tends to facilitate local exploration. [5]

r_1 and r_2 : are random numbers, which are used to maintain the diversity of the population, and are uniformly distributed in the interval [0,1]

c_1: is a positive constant, called as coefficient of the self-recognition component;

c_2: is a positive constant, called as coefficient of the social component. [6]

According to the above description about the PSO, the pseudo code of the PSO is described as follow:

```
For each particle
Initialize particle
End For
Do until maximum iterations or minimum error criteria
        For each particle
        Calculate Data fitness value
        If the fitness value is better than pBest then Set pBest = current fitness value
        If pBest is better than gBest Then Set gBest = pBest
        End For
        For each particle
        Calculate particle Velocity
        Use gBest and Velocity to update particle Data
        End For
```

The stopping condition depends on the type of problem being solved. Usually the algorithm is run for a fixed number of iterations or until a specified error bound is reached.

SEMINAL WORKS

Mid-Og Park and all proposed in **2004** in their article "Modified A5 / 1 stream cipher using S-boxes" another strategy to strengthen security of the A5 / 1 stream cipher using 4x16 s-boxes. The results show that the proposed model has the best characters of random and serial correlation if we compared to the classical version of the A5 algorithm. [7]

In **2011**, **Nikesh B** has proposed two techniques to enhancing security in A5/1 algorithm by analyzing it with different settings. The improvement was made in two ways, the first in the feedback mechanism that was reinforced by using variable valve which increases the complexity of the algorithm and the second in the shift function rules of different registers. He decreases the probability that an LFSR (R1, R2 or R3) will be shifted to 50% which was 75%. [8]

Rosepreet Kaur and **Nikesh Bajaj** [9] proposed in **2012** a modified version of A5/1 fast and easier to implement. The quality of bit stream produced by the generator was analysis by statistical tests given by national institute of standards and technology (NIST). The proposed structure includes minor increase in hardware by converting LFSR to NLFSR and change in combining function for feedback polynomials.

Darshana Upadhyay and **all** proposed in their paper "Randomness analysis of A5 / 1 stream cipher for secure mobile communications", published in March **2014** a new approach to improving A5 / 1, the strongest encryption algorithm among all the cryptographic algorithms used in mobile phone communication. They presented a cryptographic system based on NLFSRs (Non Linear Feedback Shift Register) instead of the LFSR using a non-linear combinatorial generator. It was observed that the proposed system is much better and stronger with a minor increase in hardware. [10]

Sadkhan S B and **Jawad N H** In **2014** and to increase the length of the generated keystream, authors in [11] proposed an Improvement of A5/1 encryption algorithm by applying a unit delay in the A5/1 algorithm. This was simulated in Simulink.

Authors in **2014** in their paper entitled LFSR Based Stream Cipher (Enhanced A5/1) [12] proposed a new version of the A5/1 algorithm use four LFSRs of length 30, 32, 29 and 37 instead of three in the conventional A5/1. Two of which are used for mutating of the main back-bone LFSR while the fourth LFSR mutates the final output. The proposed algorithm is simulated by using MATLAB and the Keystream generated was been have been tested using Randomness Test Suit given by National Institute of Standard and Technology (NIST). The results show that the proposed scheme is robust and resistive to the cryptographic attacks as compared to the conventional A5/1 stream cipher.

Siti Yohana Akmal Mohd Fauz & **all** in **2015** observe that the XOR function used in the conventional A5/1 contribute to the weakness of the stream cipher generated as it can be easily linearly cryptanalyzed. The authors proposed a new design which is based on a multiplexer (Mux) as opposed to the XOR combinational function. The design is programmed and simulated using C++ and the generated keystream was checked for its randomness using the NIST test suite who showed that the new design present a good alternative to enhancing the strength of the stream cipher generated. [13]

Hala Bahjat and **Mohanad Ali** in **2016** introduced new improvements to the encryption algorithm A5/ 1 stream cipher to overcome some weaknesses that appear in the shift control mechanism used in this one. They use S-box to increasing the efficiency of the majority function of the A5 / 1 algorithm and improve the randomness characteristics. [14] In their proposed scheme, it is observed that the register is shifted much better and the ciphertext of the proposed algorithm has more complexity when compared with the ciphertext of the original A5/1.

In **2017**, **Ria Elin Thomas** & **all** propose a new enhanced version of A5/1 called E-A5/1 to improve the security provided by the A5/1 algorithm. Their approach consists of xoring the key stream generated with a pseudo random number without increasing the time complexity. [15] The proposed algorithm is inexpensive because it does not need any extra hardware requirements.

OUR CONTRIBUTION: A5/PSO

As the conventional A5/1 algorithm, the A5/PSO algorithm define the taps bits of R1 at positions 13,16,17,18, and the taps of R2 are at positions 20, 21, while the taps of register R3 are in positions 7,20,21,22.

Each particle or register has a single clocking bit in position 8 for R1, 10 for R2 and R3. The output which present 228 bits of the keystream is generated by xoring the most significant bits of each register. To overcome the problems in the clocking mechanism of A5/1 and to increase its complexity, In the A5/PSO we introduce a new clocking mechanism to control the clocking of registers in the last step of the algorithm where the key stream is produced. The clocking mechanism of our proposed scheme based PSO contain two rules: the majority rule and the PSO rule.

Table 1: Comparison between the Original A5/1 and A5/PSO

	Original A5/1	**A5/PSO**
Inputs	Kc, Fn	Kc, Fn , Fitness Function
Outputs	228 bits	228 bits
Clocking Rule	Majority Rule	Majority Rule
Quality Rule	-	PSO Rule

The **Majority Rule** which consist that a register can be clocked according to the majority function M which present the majority of the clocking bit of each register R1[8], R2[10] and R3[10] and any register that its clocking bit equals to M mush be clocked.

The **PSO Rule** where any register present a particle and its can be clocked or not according to an objective function that favorite the random characteristic of the keystream produced by the algorithm.

The main of any optimization algorithm is to minimize or maximize an objective function. The optimization problem considered here is to maximize the randomness of the key stream generated by our generator called A5/PSO. Unlike the other computation techniques, each

particle in PSO has a velocity and its moves in the search space and adjusts its velocity dynamically according to its previous behaviors.

In our proposed stream cipher each register present a particle and the velocity of each particle is the number of times which the register will be shifted. Register which will be shifted with a high speed means that its values are not really random so it has to be shifted several times in order to be able to change its values rapidly. A register that will be shifted with a small speed means that its behavior is nearer to the random.

According to the above description about the PSO, the procedure of the A5/PSO is described in the following steps:

Input: 64 of the Ciphering Key **Kc**, 22 bits of the Frame Number **Fn** and The Fitness Function **F**

Output: 228 bits of the Keystream

Step 1: Initialization

- Initialization of all registers to zero
- Initialization of Kc and Fn
- Initialization of particles where each particle is presented by one register of the conventional A5/1 as follow P1=R1, P2=R2, P3=R3
- Define the Fitness Function $F= \sum Pvalue_i / N$; where i=1...N and N is the number of statistical Test

Step2: introducing Kc

- The 64 bits of the key Kc are interred by XORing each bit with the feedback bit calculated for each register by using its taps values.
- registers are clocked regularly

Step3: introducing Fn

- The 22 bits of the key Fn are interred by XORing each bit with the feedback bit calculated for each register by using its taps values.
- registers are clocked regularly

Step4: Warm up: Clock for 100 cycles and discards the output according to the Majority Rule

For i=1 to 100 do
Calculate M= Majority (R1 [8], R2 [10], R3 [10]))
If (R1 [8] =M) then clock R1
End if
If (R2 [10] =M) then clock R2
End if
If (R3 [10] =M) then clock R3
End if
End for
Step 5: Execution: Clock for 228 cycles to generate 114+114 bits according to the PSO Rule

For each particle Pi: Calculate Fitness F_{RI}
Unitizing each particle Pi best fitness by: $PBest_{Ri}=F_{Ri}$
Initialized **gBest** = the higher value of (F_{R1}, F_{R2}, F_{R3})
Initializing all velocities V_{R1}, V_{R2}, V_{R3} of all particles P1, P2, P3 to zero
For J=1 to 228 do
Calculate **F**= Fitness (Key stream+ (R1 [19] ^ R2 [22] ^ R3 [23]))
If (**F > gBest**) clock all registers irregularly according to the majority Rule and produce one bit of the Keystream
Else
For i=1 to 3 do
For each particle $P_{I:}$ Calculate Fitness F_{Ri}
Update $pBest_{Ri}$: if (F_{Ri} > $pBest_{Ri}$) then $pBest_{Ri}$= F_{Ri} end if
End for
Update gBest
For I=1 to 3 do
Calculate the Velocity of each register using the equation
$V_{RI}= V_{RI}+C1 X Rand1 X (pBest_{RI} - F_{Ri}) + C2 X Rand2 X (gBest - F_{Ri})$
End for
Shift each register according to its velocity V_{RI} and produce one bit of the keystream
End if
End for.

PERFORMANCE EVALUATION OF A5/PSO

The table below presents a comparison between some previous works were the authors have tried to improve the security of the mobile telecommunication networks and more particularly to enhance the security of the conventional A5/1 which ensures the confidentiality of the data exchanged in the air interface between the mobile device and the network.

Table 2: Comparison between Some Enhanced Versions of A5/1

Ref	Year	Algorithm	Hardware Change	Time Complexity	Approach	Quality Factor
A5/1	1999	A5/1	-	-	Majority Rule	No
[7]	2004	-	Major	High	S-boxes	NO
[8]	2011	Enhanced A5/1	Major	High	Feedback Mechanism+ M Rule	No
[9]	2012	-	Minor	LOW	NLFSR+ Majority Rule	No
[10]	2014	-	Medium	Medium	NLFSR	No
[11]	2014	-	Minor	LOW	Unit delay+ Majority Rule	No
[12]	2014	Enhanced A5/1	Major	High	4 LFSR+ Majority Rule	No
[13]	2015	-	Minor	LOW	MUX + Majority Rule	No
[14]	2016	-	Major	High	S-box + Majority Rule	No
[15]	2017	E-A5/1	Minor	LOW	XOR+ Majority Rule	No
OUR	2019	A5/PSO	Minor	LOW	Majority Rule	PSO Rule

Almost of these proposal approach have tried to overstate the different weaknesses presented in the standard version of the A5/1 including the size of the key and the function that manages the clock of the different registers that compose A5/1.

Some authors have attempted to use NLFSR instead of LFSR, others have directed to use sboxes to improve the security of the mobile phone cryptosystem, and while others have tried to increase the number of registers composes A5/1 or to implement a control unit jointly with the majority function to better manage the shift operations of the different registers compose the A5/1 stream cipher.

Unfortunately none of these approaches includes a mechanism that guarantees the quality of the generated keystream and the majority if not all of authors use the NIST statistical tests to check the quality of the generated keystream. Even if keysteam has a good quality, the majority of the authors do not discuss the initialization parameters of their enhanced versions of the A5/1 algorithm because a little change in these parameters including Kc and the Fn can influence vitally on the quality generated keystream.

A5/PSO presents another vision to enhance the security of the conventional A5/1 generator to make it more secure, complex and resistant to some known attacks. Our approach integrates a small mechanism that intelligently controls a shifting of the different registers R1, R2 and R3 that compose A5/1. This new function is based on an optimization algorithm known as Particle Swarm Optimization Algorithm.

SECURITY ANALYSIS OF A5/PSO

The A5/1 algorithm is massively deployed, but does not offer absolute privacy protection. A5/1 has been cryptanalysed and several attacks against A5/1 have been published since the late 1990.

Guess and Determine Attacks

Guess and determine attack was applied to A5/1 by **Anderson** in **1994** in which he proposed to guess all bits of registers R1 (19 bits) and R2 and 11bits of R3 (22 bits) to determine the initial state of the generator where the attacker will search about $\mathbf{2^{52}}$ (19+22+11=52) cases to determine the correct unknown bits of R3. [16]

Later in **1997**, **Golic** [17] proposed an attack of the algorithm A5/1 based on a resolution of a system of equations where first, half of initial values for all registers R1, R2, and R3 have been guessed to determine values of these registers based on information extracted from known keystream by solving the set of 64x64 linear equations. The complexity of the attack was about $\mathbf{2^{40}}$ and require solving more than 40 linear equations by Gaussian Elimination method.

In our A5/PSO a new clock control mechanism is proposed to increase the complexity of the algorithm. This new mechanism is not based just only in the majority function that takes three input bits (R1 [8], R2 [10], R3 [10]) and produces a single output bit. The new PSO rule used in our approach needs all values of all registers to produce a bit output. Guessed a small number of bits do not seem enough to be able to make an attack.

In **2014**, an improved version of Guess and Determine attack against A5/1 cipher has been presented by **Mahalanobis & Shah** [18] required about $\mathbf{2^{48.5}}$. Firstly and with 64 bits of the keystream that will be available for cryptanalyst, 19 bits of register R1 are guessed, and then the initial values of registers R1 and R2 will are determined in the second steps. After that a set of states will be built or each new state designates a candidate generator. Each generator will be launched to produce a set of bits that will be compared later with the 64 bits of keystream available. If the outputs of the candidate generator matching with the Keystream available, then the initial values of registers R1, R2, and R3 represent the values of the secret key sought.

The attack was presented in two phases, determination phase and post processing phase. The determination phase is decomposed also in two phases or the first phase named Processing Phase1 that compute the most significant bits of register R2 and R3 using the most significant bits of register R1 and the available keystream bits. The second phase was called as processing phase2 which consider the clocking bits of registers R2 and R3.

Table 3: Complexity of Some Guess and Determine Attacks of A5/1

Attack	Bits Guessed	Keystream Available	Complexity
Anderson	52 bits	0 bits	$\mathbf{2^{52}}$
Golic	32 bits	0 bits	$\mathbf{2^{40}}$
Mahalanobis & Shah	19 bits	$\mathbf{2^6}$=64 bits	$\mathbf{2^{48.5}}$

The attack has a 100% success rate and requires about 5.65 GB storage. The attack is based on the weakness of the majority function used to clock the registers R1, R2 and R3. With every additional clocking round, the number of complete state candidates that contain the real key increases and consequently the probability of finding the key among all the complete state candidates increases with every additional round after 11 clocking rounds.

In A5/PSO the keystream is generated in the last step of the algorithm that produces 228 bits of the keystream by applying the PSO Rule. Concerning the first phase of determination, there is not a possibility to determine the bits of the register R2 and R3 from a few bits of the Keystream available for the attacker because the PSO Rule required that all values of all registers R1, R2, R3 be known. Secondly, even if an attacker builds a list of complete states candidates, he does not know the criterion of optimization carried by the PSO Rule, we are talking here about the fitness function assigned to the PSO Rule, since this fitness function is never interchanged between the mobile station and the network. For all these reasons, the complexity of this attack is $\mathbf{2^{64}}$.

Table4: Resistance of A5/1 to Some Known Guess and Determine Attacks

	Original A5/1		*A5/PSO*	
Attack	**Bits Guessed**	**Complexity**	**Bits Guessed**	**Complexity**
Anderson	52 bits	$\mathbf{2^{52}}$	64 bits	$\mathbf{2^{64}}$
Golic	32 bits	$\mathbf{2^{40}}$	64 bits	$\mathbf{2^{64}}$
Mahalanobis & Shah	19 bits	$\mathbf{2^{48.5}}$	64 bits	$\mathbf{2^{64}}$

Correlation and Time Memory Trade of Attacks

In contrast to time memory trade of attacks, **Patrik Ekdahl** and **Thomas Johansson** in **2002** authors propose a new correlation attack of A5/1 encryption algorithm that explores the weak key initialization that separates the session key from the frame number. [19]The attack has a high success rate which was more than 70% and the complexity of the attack is only linear in the length of the shift registers and depends instead on the number of irregular clocking before the keystream is produced. The attack suggests 40 first bits from about 2^{16} frames, which corresponds to about 5minutes of GSM conversation plaintext.

In **2001**, **Biryukov** & **all** have presented an improved time memory trade off attacks called biased birthday attack [20]. The main idea of this attack is to consider sets A and B which are not chosen through the uniform probability distribution among all the possible states. The reason which makes this attack efficient is that in the standard GSM A5/1, the register bits that affect the clock control and the register bits that affect the output are unrelated for about 16 clock cycles. This decreases the state ($2^{64}=2^{19}+2^{22}+2^{23}$) to be sampled to $\mathbf{2^{48}}=2^{64}-2^{16}$.

These attacks explore essentially the weaknesses posed by the use of the majority function in the original A5/1 algorithm. These attacks cannot be applied on our new improved version of the A5/1 named A5/PSO because the weaknesses of this so-called majority function which handles the shifting of the original A5/1 registers is improved by the use of a new function which is based on a criterion of optimization using particle Swarm Optimization Algorithm.

CONCLUSION

Cellular networks must more than ever meet security requirements to best ensure the various security objectives including confidentiality, integrity and availability. Several articles have been published in recent years aiming to improve security in mobile telephone networks and more particularly that propose improvements to the series of algorithms ensuring the confidentiality of mobile communications named A5 whose version A5/1 is the most robust but none of these approaches incorporates a mechanism to control the quality of the keystream generated by their pseudo-random generators. By the way, the majority of authors, if not all, use NIST tests to be able to validate and ensure the quality of the keystream generated with a limited number of initialization parameters, or the authors will not discuss it in the majority of cases. Because such a generator can give good quality pseudo-random sequences with certain initialization parameters but the quality may be degraded while using other initialization parameters.

This paper is initiated to a new class of pseudo random generators where the quality of the generated sequences is guaranteed. Our approach is based on optimization algorithms known as Particle Swarm Optimization Algorithm that have been used in this article to improve security in mobile networks. In this paper, a new version of the A5/1 stream cipher called A5/PSO has been proposed to improve the randomization property of A5/1 algorithm to make it robust and resistive to some known attacks.

After the analysis of the different results, it has been shown that proposed stream cipher has improved the randomness performance because of the good characteristic of randomness of the output bit stream generated by the enhanced scheme. A security analysis also of the new scheme confirm that it is very secure and have more strengthen if we compared with the

conventional ciphering algorithm A5/1. This type of generator is a very good initiative to build new pseudo random generators where the quality of the generated keystream guaranteed by the same generator.

REFERENCES

[1] A. Biryukov, A. Shamir, D. Wagner, (2000) Real Time Cryptanalysis of A5/1 on a PC, Fast Software Encryption Workshop 2000, New York, USA, April 10-12.

[2] S. Babbage, (May 1995)A Space / Time Tradeoff in Exhaustive Search Attacks on Stream Ciphers, European Convention on Security and Detection, IEE Conference publication, No 408,.

[3] S.E.AlAschkar and M.T.El-Hadidi, Known attacks for the A5/1 algorithm: A Tutorial, International Conference on Information and Communications Technology (ICICT03), pp. 229-251, 2003

[4] Chia-Chong Chen , (2009) Hierarchical Particle Swarm Optimization for Optimization Problems, Tamkang Journal of Science and Engineering, Vol. 12, No. 3, pp. 289298

[5] Shahriar ASTA, A Novel Particle Swarm Optimization Algorithm, Thesis, Istanbul Technical University Graduate School of Science Engineering and Technology.

[6] Ismail K. Ali , Abdulelah I. Jarullah, (January 2012) A New Keystream Generator Based on Swarm Intelligence, Diyala Journal For Pure Sciences, Vol: 8 No: 2, April 2012

[7] Mi-Og P , C.Yeon-Hee, J. Moon-Seog.(February 2004). Modified A5/1Stream Cipher using S-boxes , The 6th International Conference on Advanced Communication Technology Vol. , pages 508-511

[8] B. Nikesh. (July 2011).Effects of Parameters of Enhanced A5/1. International Journal of Computers and Applications IJCA Special Issue on Evolution in Networks and Computer Communications

[9] Rosepreet Kaur, Nikesh Bajaj. (November 2012). Enhancement in Feedback Polynomials of LFSR used in A5/1 Stream Cipher. International Journal of Computer Applications. Vol.57, No.19.

[10] Darshana Upadhyay, Priyanka Sharma, Sharada Valiveti .(September 2014).Randomness analysis of A5/1 Stream Cipher for secure mobile communication. International Journal of Computer Science & Communication, Vol.5, No.1, page 95-100.

[11] Sadkhan S B and Jawad N H (2014). Improvement of A5/1 Encryption Algorithm Based on Using Unit Delay. Iraqi Academic Scientific Journal 22 622–63

[12] Amandeep Singh Bhal, Zhilmil Dhillon.(December 2014) LFSR BASED STREAM CIPHER (ENHANCED A5/1), International Journal of Advanced Computational Engineering and Networking, ISSN: 2320-2106 Vol.2, No.12

[13] Siti Yohana Akmal Mohd Fauzi, Marinah Othman, Farrah Masyitah Mohd Shuib and Kamaruzzaman Seman, (September 2015) An Enhanced A5/1 Stream Cipher Utilising An Improved combinational Function For GSM Communication, Proceeding of The Third International Conference en Intelligence and Computer Sciences AICS2015, Malaysia,

[14] Hala Bahjat, Mohanad Ali, (2016). Improvement Majority Function in A5/1 stream cipher Algorithm. International Journal of Engineering & Technology, Vol.34 No.1

[15] Ria Elin Thomas, G Chandhiny, Katyayani Sharma, H Santhi and P Gayathri. (2017). Enhancement of A5/1 encryption algorithm. IOP Conference Series: Materials Science and Engineering. 263. 042084. 10.1088/1757-899X/263/4/042084.

[16] R. Anderson, (1994) A5 (was: Hacking digital phones) , Newsgroup Communication

[17] J. Golic, (1997) Cryptanalysis of alleged A5 stream cipher, Advances in Cryptology, proceedings of EUROCRYPT'97, LNCS, vol. 1233, pp.239–255, Springer-Verlag, 1997

[18] Ayan Mahalanobis, Jay Shah, (2014) An Improved Guess-and-Determine Attack on the A5/1 Stream Cipher, Computer and Information Science; Vol. 7, No. 1.

[19] P. Ekdahl, and T. Johansson, (2003) Another attack on A5/1, IEEE Transactions on Information Theory, vol. 49, pp. 284-289.

[20] A. Biryukov, A. Shamir, and D. Wagner, (2001) Real time cryptanalysis of A5/1 on a PC, Advances in Cryptology,proceedings of Fast Software Encryption'00,LNCS,pp.1–18,Springer-Verlag.

Manuscript submitted to :
SECOND INTERNATIONAL WORKSHOP ON CRYPTOGRAPHY AND ITS APPLICATIONS: 2 IWCA 19.
Organised by l'USTO-MB 22-23 April 2019 U.S.T.O-MB, ORAN, ALGERIA.

Nonstandard notes on the ratio of two expressions formed by the product and the sum of certain multiplicative arithmetic functions

DJAMEL BELLAOUAR

ABSTRACT. In the framework of internal set theory (IST) any real number must be infinitesimal, appreciable or unlimited. For instance, such numbers are called standard or nonstandard. Let E be an infinite external subset of positive integers and let f and g be two expressions formed by the product and the sum of certain multiplicative arithmetic functions. In this paper, we prove the existence of infinitely many positive integers $n \in E$ such that $\frac{f(n)}{g(n)}$ is equivalent to a nonstandard number.

1. INTRODUCTION

Historically one finds that Leibniz, Euler and Cauchy are the first who began the use of infinitely small quantities. The absence of rigor surrounding the use of this notion found solution after an approach due to Abraham Robinson in 1961. In 1977 Edward Nelson provided another presentation of the nonstandard analysis, called IST (Internal Set Theory), based on ZFC to which is added a new unary predicate called "standard". The use of this predicate is governed by the following three axioms: Transfer principle, Idealization principle and Standardization principle. For details, see [12], [14]. Formulas that involve the predicate st are called external, the others are called internal and correspond to formulas of conventional set theory. We can freely use the terms such as external function, external sequence corresponding to external formulas or internal function, internal sequence corresponding to internal formulas.

Any real number that can be characterized in unique classical way is necessarily standard. Thus, $0, 1, ...\sqrt{2}, \pi, 10^{10000}, ...$ are standard. But are not all reals therefore standard. A real number ϵ is called infinitesimal if for all standard numbers $n \in \mathbb{N}$, one has $|\epsilon| < \frac{1}{n}$. A real number ω is called unlimited or infinitely large if $|\omega| > n$, for all standard $n \in \mathbb{N}$. Non-zero infinitesimals and unlimited numbers are nonstandard. Thus, a real number r is called limited if is not unlimited and appreciable if it is neither unlimited nor infinitesimal. In addition, two real numbers x and y are equivalent or infinitely close, denoted by $x \simeq y$, if their difference $x - y$ is infinitesimal.

An internal set is a collection of mathematical entities defined by an internal formula. For example, let $\varepsilon > 0$ be an infinitesimal, the collection of real numbers $\{x \in \mathbb{R} : |x| \leq \varepsilon\}$ is an internal set but not a standard set. IST only deals with internal sets. Moreover, the collection of all infinitesimals $\oslash = \{\epsilon \in \mathbb{R} : \epsilon \simeq 0\}$ is not an internal set. More examples of external sets are the set of all positive unlimited numbers, denoted by ∞, the set of

Received: 15 th January 2019.
2010 *Mathematics Subject Classification.* 11A25, 11J25, 03H05.
Key words and phrases. *Multiplicative functions, prime numbers, Diophantine inequalities, Internal Set Theory.*
Corresponding author: Djamel BELLAOUAR. Email: bellaouar.djamel@univ-guelma.dz

all limited numbers, denoted by $\pounds$, which are real numbers but not unlimited numbers, or the set of all appreciable positive numbers, denoted by @, which are positive limited numbers that are not infinitesimal. Of course, the set of limited positive integers, denoted by $\mathbb{N}^{\sigma}$, is an external subset of $\mathbb{N}$.

Some researchers have studied the application of Nonstandard Analysis in several domains of mathematics. For example, one can see [4],[5],[8],[9],[15]. In the present paper, by using external subsets of positive integers we will study Diophantine equations of the form

$$\frac{f(n)}{g(n)} \simeq a, \tag{1.1}$$

where f and g are two arithmetic functions and a is a nonstandard number. Equations of the form (1.1) we can call them external Diophantine equations. This name comes from the fact that $\frac{f(n)}{g(n)}$ equivalent to a, i.e., $\frac{f(n)}{g(n)}$ is very near to a within the meaning of the theory of IST, that is, an external formulation. In fact, in this paper we prove the equation (1.1) for infinitely many unlimited n.

Let us define for the natural number $n \geq 2$:

$$n = \prod_{i=1}^{a} q_i^{\alpha_i}, \tag{1.2}$$

where a, $\alpha_1, \alpha_2, \ldots, \alpha_a$ are positive integers and $q_1, q_2, ..., q_a$ are different primes, the following functions

1. Let $s \geq 1$. The generalized Euler phi function $\varphi_s(n)$ and the generalized Dedekind function $\psi_s(n)$ are given by
$$\varphi_s(n) = n^s \prod_{i=1}^{a} \left(1 - \frac{1}{q_i^s}\right) \text{ and } \psi_s(n) = n^s \prod_{i=1}^{a} \left(1 + \frac{1}{q_i^s}\right),$$
respectively, where $\varphi_s(1) = \psi_s(1) = 1$. For $s = 1$, φ_1 is denoted by φ and ψ_1 is by ψ.
2. The divisor function $\tau(n)$ counts the number of positive divisors of n. That is, $\tau(n) = \sum_{d|n} 1$. Hence by (1.2),
$$\tau(n) = \prod_{i=1}^{a} (\alpha_i + 1).$$
3. $\omega(n)$ is the number of distinct prime factors of n. In view of (1.2), $\omega(n) = a$.

In the present paper, we shall continue the research from [3]. In fact, let k be a positive integer and let W_k denote the set of positive integers n for which the number of distinct prime factors of n is larger or equal to k. Let E be an infinite external subset of W_k and let f and g be two expressions formed by the product and the sum of certain multiplicative arithmetic functions such as φ_s, ψ_s, τ and ω. It is naturel to ask the following general question: Are there infinitely many $n \in E$ such that

$$\frac{f(\varphi_s(n), \psi_s(n), \tau(n), \omega(n))}{g(\varphi_s(n), \psi_s(n), \tau(n), \omega(n))} \simeq a, \tag{1.3}$$

where a is a given nonstandard number? In this work, we shall present some notes to answer this question.

Finally, recall that functions, sequences and equations which involve additive convex subgroups are called flexible. For details, see [9]. Similar to Equations (1.1) and (1.3), we can show that $\frac{f}{g}$ can be a flexible multiplicative function when we define it using special convex additive subgroups of $\mathbb{R}$, which are external subsets.

2. MATERIALS

Before launching the proof of our main results, we present some notions and results on the prime numbers and internal set theory that we shall use later. For more details, see [2],[7],[12], [13],[15].

Conjecture 1 (Dickson's conjecture)**.** *Let $s \geq 1$, $f_i(x) = b_i x + a_i$ with a_i, b_i integers, $b_i \geq 1$ (for $i = 1, 2, ..., s$). Dickson's conjecture* [13] *says that, if there is no fixed integer greater than one which divides*

$$f(x) = f_1(x) f_2(x) \cdots f_n(x)$$

for all integers x, then $f_1(x), \ldots, f_n(x)$ are simultaneously prime for infinitely many values of x.

Theorem 2.1 ([4])**.** *Assuming the Dickson Conjecture, for each couple of integers $q > 0$ and $k > 0$, there exists an infinite subset $L_{q,k} \subset \mathbb{N}$ such that for every $n \in L_{q,k}$ and for every $l \in [-q, q]$ with $l \neq 0$, one has*

$$n + l = |l|\, t_1 t_2 ... t_k \ ,$$

where $t_1 < t_2 < ... < t_k$ are prime numbers. Further, for each couple of integers $q > 0$ and $k > 0$, there exists an infinite subset $M_{q,k} \subset \mathbb{N}$ such that for every $n \in M_{q,k}$ and for every $l \in [-q, q]$, one has

$$n + l = r t_1 t_2 ... t_k,$$

where $t_1 < t_2 < ... < t_k$ are also prime numbers and $r \in [1, 2q + 1]$.

Let p_n be the n-th prime number with $n \geq 2$. We denote by d_{n-1} the gap between p_n and p_{n-1}, that is, $d_{n-1} = p_n - p_{n-1}$. Using the Prime Number Theorem, it is well known that

$$\lim_{n \to +\infty} \frac{p_n}{d_n} = +\infty. \tag{2.4}$$

Let $k \geq 1$ and let W_k be the set as stated in the introduction ($n \in W_k$ means that n is a positive integer and $\omega(n) \geq k$). By (2.4), we can easily choose two positive integers r and s with $r \geq 4$ such that

$$p_k < \left(1 + \frac{p_{r-1} - 1}{d_{r-1} + 1}\right)^{\frac{1}{s}}. \tag{2.5}$$

Then we have.

Theorem 2.2 ([2])**.** *Under the same assumption as in* (2.5)*, $\varphi_s(n) - a_r n^s$ has infinitely many sign changes on the set W_k, where $a_r = \frac{p_{r-1}}{p_r}$.*

Thus, if (2.5) holds for some k, r and s, then there are infinitely many $n \in W_k$ such that $\frac{\varphi_s(n)}{n^s} > a_r$ and there are infinitely many $m \in W_k$ such that $\frac{\varphi_s(m)}{m^s} < a_r$.

Theorem 2.3 (see [15]). *Let $(u_n)_{n\geq 1}$ be a standard sequence of elements of $\mathbb{R}$. Then $(u_n)_{n\geq 1}$ converges to l if and only if $u_n \simeq l$ for all unlimited n.*

Remark 2.1. In the case when s is limited and r is unlimited, then by (2.4) and Theorem 2.3, any limited (standard) prime number satisfies (2.5).

Notation 1. We denote by L_∞ the subset of positive integers given by

$$L_\infty = \{n = p_1^{\alpha_1} p_2^{\alpha_2} ... p_k^{\alpha_k} / \ \alpha_i \geq 1, \text{for } i = 1, 2, ..., k \text{ with } k \simeq +\infty\},$$

where $2 = p_1 < p_2 < ...$ is the sequence of all primes in ascending order.

Notation 2. Define

$$W_\infty = \left\{n = p_{i_1}^{\alpha_1} p_{i_2}^{\alpha_2} ... p_{i_s}^{\alpha_s} \in \mathbb{N} \, ; \, s \simeq +\infty \text{ and } p_{i_j} \simeq +\infty, \text{for } j = 1, 2, ..., s\right\}.$$

Note that for any standard $k \geq 1$, W_∞ is a proper subset of W_k.

Example 2.2. Let p be an unlimited prime number, then $2.3.5....p \in L_\infty$. Further, if N is an unlimited positive integer, then

$$p_N p_{N+1} ... p_{2N} \in W_\infty.$$

Definition 2.1 (see, [7]). Let X be a standard set, and let $(A_x)_{x\in X}$ be an internal family of sets:

a. A union of the form $G = \bigcup\limits_{stx\in X} A_x$ is called a *pregalaxy*; if it is external G is called a *galaxy*.
b. An intersection of the form $H = \bigcap\limits_{stx\in X} A_x$ is called a *prehalo*; if it is external H is called a *halo*.

Example 2.2 (for details, see [2]). We have

1. The set $\mathbb{N}^\sigma$ is a galaxy.
2. The set $\oslash = \{\epsilon \in \mathbb{R} : \epsilon \simeq 0\}$ is a halo.

The following two principles are important in order to separate some cases where the solution of a given Diophantine inequality has adjacent factors. For example when the solution is of the form $n = 2.3.5...p$, where $p \simeq +\infty$.

Theorem 2.4 (Cauchy's Principle,[7, p.19]). *No external set is internal.*

Theorem 2.5 (Fehrele's Principle,[7, p.20]). *No halo is a galaxy.*

We also denote by $\oslash$, @, $\pounds$ and ω the real number which is infinitesimal, appreciable, limited and unlimited, respectively [7].

Our main results are as follows.

3. Main results

In 2011, T. Krassimir [10] established the following theorem: For each natural number $n > 1$,

$$\varphi(n)^{\varphi(n)} \psi(n)^{\psi(n)} > n^{2n}.$$

We prove below a similar external result.

Theorem 3.6. *Let s be a limited positive integer. Assuming Dickson's conjecture, there are infinitely many n such that*

$$\frac{\varphi_s(n)^{\frac{\varphi_s(n)}{\psi_s(n)}}\,\psi_s(n)^{\frac{\psi_s(n)}{\varphi_s(n)}}}{n^{2s}} \simeq +\infty.$$

Proof. Let k, q be limited positive integers and let $L_{q,k}$ be the infinite subset defined in Theorem 2.1. It suffices to prove that

$$\frac{\varphi_s(n+l)^{\frac{\varphi_s(n+l)}{\psi_s(n+l)}}\,\psi_s(n+l)^{\frac{\psi_s(n+l)}{\varphi_s(n+l)}}}{(n+l)^{2s}} \simeq +\infty,$$

for every unlimited $n \in L_{q,k}$ and for every integer l with $0 < l \leq q$. In fact, let $n \in L_{q,k}$ be unlimited. Assume that $n + l = lt_1t_2...t_k$, where $0 < t_1 < t_2 < ... < t_k$ are primes and $0 < l \leq q$. Since k is limited, then we distinguish two cases.

1. In the case when $t_i \simeq +\infty$, for $i = 1, 2, ..., k$. Since $(l, t_1t_2...t_k) = 1$ because l is

standard, it follows that

$$\begin{aligned}
&\frac{\varphi_s(n+l)^{\frac{\varphi_s(n+l)}{\psi_s(n+l)}}\,\psi_s(n+l)^{\frac{\psi_s(n+l)}{\varphi_s(n+l)}}}{(n+l)^{2s}} \\
= \;& \frac{\varphi_s(lt_1t_2...t_k)^{\frac{\varphi_s(lt_1t_2...t_k)}{\psi_s(lt_1t_2...t_k)}}\,\psi_s(lt_1t_2...t_k)^{\frac{\psi_s(lt_1t_2...t_k)}{\varphi_s(lt_1t_2...t_k)}}}{(lt_1t_2...t_k)^{2s}} \\
\simeq \;& @.\frac{[(t_1^s-1)...(t_k^s-1)]^{\frac{\varphi_s(l)}{\psi_s(l)}\frac{(t_1^s-1)...(t_k^s-1)}{(t_1^s+1)...(t_k^s+1)}}\,[(t_1^s+1)...(t_k^s+1)]^{\frac{\psi_s(l)}{\varphi_s(l)}\frac{(t_1^s+1)...(t_k^s+1)}{(t_1-1)...(t_k-1)}}}{(t_1t_2...t_k)^{2s}},
\end{aligned}$$

where

$$@ = \frac{\varphi_s(l)^{\frac{\varphi_s(l)}{\psi_s(l)}}\,\psi_s(l)^{\frac{\psi_s(l)}{\varphi_s(l)}}}{l^{2s}}.$$

We put

$$\alpha_s(l) = \frac{\varphi_s(l)}{\psi_s(l)} + \frac{\psi_s(l)}{\varphi_s(l)}$$

and

$$\omega = \frac{[(t_1^s-1)...(t_k^s-1)]^{\frac{\varphi_s(l)}{\psi_s(l)}\frac{(t_1^s-1)...(t_k^s-1)}{(t_1^s+1)...(t_k^s+1)}}\,[(t_1^s+1)...(t_k^s+1)]^{\frac{\psi_s(l)}{\varphi_s(l)}\frac{(t_1^s+1)...(t_k^s+1)}{(t_1-1)...(t_k-1)}}}{(t_1t_2...t_k)^{2s}}. \tag{3.6}$$

It is clear that @ is appreciable, since l and s are limited. Moreover, by simple computation we obtain

$$\begin{aligned}
\alpha_s(l) &= \frac{\prod_{p|l}\left(1-\frac{1}{p^s}\right)}{\prod_{p|l}\left(1+\frac{1}{p^s}\right)} + \frac{\prod_{p|l}\left(1+\frac{1}{p^s}\right)}{\prod_{p|l}\left(1-\frac{1}{p^s}\right)} \\
&= 2\prod_{p|l}\frac{p^{2s}}{p^{2s}-1} + \frac{\text{a positive integer}}{\prod_{p|l}p^{2s}-1} = 2 + r, \qquad (3.7)
\end{aligned}$$

where r is standard rational number less than 1. Also, it follows from (3.6) that

$$\begin{aligned}
\omega &> \frac{\left[\left(t_1^s-1\right)\left(t_2^s-1\right)...\left(t_k^s-1\right)\right]^{(2+r)\frac{\left(t_1^s-1\right)...\left(t_k^s-1\right)}{\left(t_1^s+1\right)...\left(t_k^s+1\right)}}}{\left(t_1t_2...t_k\right)^{2s}} \\
&= \frac{\left[\left(t_1^s-1\right)\left(t_2^s-1\right)...\left(t_k^s-1\right)\right]^{2+@'}}{\left(t_1t_2...t_k\right)^{2s}} \\
&= \frac{\left(t_1^s-1\right)^2\left(t_2^s-1\right)^2...\left(t_k^s-1\right)^2}{\left(t_1t_2...t_k\right)^{2s}}\left(t_1^s-1\right)^{@'}\left(t_2^s-1\right)^{@'}...\left(t_k^s-1\right)^{@'} \\
&\simeq \left(t_1^s-1\right)^{@'}\left(t_2^s-1\right)^{@'}...\left(t_k^s-1\right)^{@'} \\
&\simeq +\infty,
\end{aligned}$$

where $@'$ is also appreciable positive with $@' \simeq r$. Therefore,

$$\frac{\varphi_s\left(n+l\right)^{\frac{\varphi_s(n+l)}{\psi_s(n+l)}}\psi_s\left(n+l\right)^{\frac{\psi_s(n+l)}{\varphi_s(n+l)}}}{\left(n+l\right)^{2s}} \simeq @.\omega \simeq +\infty.$$

2. In the case when t_i is standard for $1 \leq i \leq i_0$ and t_i is unlimited for $i_0 < i \leq k$. Since $n+l = lt_1t_2...t_{i_0}t_{i_0+1}...t_k$ and $\left(lt_1t_2...t_{i_0}, t_{i_0+1}...t_k\right) = 1$, then from the previous case we have

$$\begin{aligned}
&\frac{\varphi_s\left(n+l\right)^{\frac{\varphi_s(n+l)}{\psi_s(n+l)}}\psi_s\left(n+l\right)^{\frac{\psi_s(n+l)}{\varphi_s(n+l)}}}{\left(n+l\right)^{2s}} \\
= &\frac{\varphi_s\left(lt_1t_2...t_{i_0}t_{i_0+1}...t_k\right)^{\frac{\varphi_s\left(lt_1t_2...t_{i_0}t_{i_0+1}...t_k\right)}{\psi_s\left(lt_1t_2...t_{i_0}t_{i_0+1}...t_k\right)}}\psi_s\left(lt_1t_2...t_{i_0}t_{i_0+1}...t_k\right)^{\frac{\psi_s\left(lt_1t_2...t_{i_0}t_{i_0+1}...t_k\right)}{\varphi_s\left(lt_1t_2...t_{i_0}t_{i_0+1}...t_k\right)}}}{\left(lt_1t_2...t_{i_0}t_{i_0+1}...t_k\right)^{2s}} \\
\simeq &@''.\frac{\left[\left(t_{i_0+1}^s-1\right)...\left(t_k^s-1\right)\right]^{\frac{\varphi_s(l')}{\psi_s(l')}\frac{\left(t_{i_0+1}^s-1\right)...\left(t_k^s-1\right)}{\left(t_{i_0+1}^s+1\right)...\left(t_k^s+1\right)}}}{\left(t_{i_0+1}...t_k\right)^{2s}} \times \\
&\left[\left(t_{i_0+1}^s+1\right)...\left(t_k^s+1\right)\right]^{\frac{\psi_s(l')}{\varphi_s(l')}\frac{\left(t_{i_0+1}^s+1\right)...\left(t_k^s+1\right)}{\left(t_{i_0+1}^s-1\right)...\left(t_k^s-1\right)}} \\
> &@''.\frac{\left[\left(t_{i_0+1}^s-1\right)...\left(t_k^s-1\right)\right]^{\left(\frac{\varphi_s(l')}{\psi_s(l')}+\frac{\psi_s(l')}{\varphi_s(l')}\right)\frac{\left(t_{i_0+1}^s-1\right)...\left(t_k^s-1\right)}{\left(t_{i_0+1}^s+1\right)...\left(t_k^s+1\right)}}}{\left(t_{i_0+1}...t_k\right)^{2s}} \\
\simeq &+\infty,
\end{aligned}$$

where $@'' = \frac{\varphi_s\left(l'\right)^{\frac{\varphi_s(l')}{\psi_s(l')}}\psi_s\left(l'\right)^{\frac{\psi_s(l')}{\varphi_s(l')}}}{\left(l'\right)^{2s}}$ and $l' = lt_1...t_{i_0}$ are appreciable. The proof of Theorem 3.6 is finished. □

On the set L_∞ we have.

Lemma 3.1. *L_∞ is an external subset.*

Proof. Let $p_1 = 2, p_2 = 3, ...$ be the sequence of all primes. From the definition of L_∞ we see that for every limited n, $p_1p_2...p_n \notin L_\infty$. If L_∞ is internal, then by Cauchy's

principle there exists an unlimited n_0 such that $p_1p_2...p_{n_0} \notin L_\infty$. This contradicts the fact that $p_1p_2...p_s \in L_\infty$ for any unlimited s. Thus, L_∞ is an external subset. □

Theorem 3.7. *For each natural number $n \in L_\infty$, one has*

$$\varphi_s(n)^{\frac{\varphi_s(n)}{\psi_s(n)}}\,\psi_s(n)^{\frac{\psi_s(n)}{\varphi_s(n)}} > n^{2s\omega_n^{2s}\phi_n},$$

where ω_n and $\pounds_n$ are certain positive constants depending only on n with $\omega_n \simeq +\infty$ and $\phi_n \simeq 0$.

Proof. Let $n = p_1^{\alpha_1}p_2^{\alpha_2}...p_k^{\alpha_k} \in L_\infty$, where $k \simeq +\infty$, $2 = p_1 < p_2 < ...$ is the sequence of all primes and $\alpha_i \geq 1$ for $i = 1, 2, ..., k$. We first show that there exists a real number $\alpha_s(n)$ with $\alpha_s(n) > 2$ such that

$$\varphi_s(n)^{\frac{\varphi_s(n)}{\psi_s(n)}}\,\psi_s(n)^{\frac{\psi_s(n)}{\varphi_s(n)}} > n^{s\alpha_s(n)}. \tag{3.8}$$

Using the properties of φ_s and ψ_s, we obtain

$$\begin{aligned}
&\frac{\varphi_s(n)}{\psi_s(n)}\ln\varphi_s(n) + \frac{\psi_s(n)}{\varphi_s(n)}\ln\psi_s(n)\\
&= \frac{\prod\limits_{p|n}\left(1-\frac{1}{p^s}\right)}{\prod\limits_{p|n}\left(1+\frac{1}{p^s}\right)}\ln\left(n^s\prod_{p|n}\left(1-\frac{1}{p^s}\right)\right) + \frac{\prod\limits_{p|n}\left(1+\frac{1}{p^s}\right)}{\prod\limits_{p|n}\left(1-\frac{1}{p^s}\right)}\ln\left(n^s\prod_{p|n}\left(1+\frac{1}{p^s}\right)\right)\\
&= \alpha_s(n)\ln n^s + \underbrace{\frac{\prod\limits_{p|n}\left(1-\frac{1}{p^s}\right)\sum\limits_{p|n}\ln\left(1-\frac{1}{p^s}\right)}{\prod\limits_{p|n}\left(1+\frac{1}{p^s}\right)} + \frac{\prod\limits_{p|n}\left(1+\frac{1}{p^s}\right)\sum\limits_{p|n}\ln\left(1+\frac{1}{p^s}\right)}{\prod\limits_{p|n}\left(1-\frac{1}{p^s}\right)}}_{\beta_s(n)},
\end{aligned} \tag{3.9}$$

where $\alpha_s(n)$ is defined as in (3.7). Therefore, $\alpha_s(n) > 2$.

Next, we prove that $\beta_s(n) > 0$. In fact, since

$$\beta_s(n) \geq \frac{\prod\limits_{p|n}\left(1-\frac{1}{p^s}\right)\sum\limits_{p|n}\ln\left(1-\frac{1}{p^s}\right) + \prod\limits_{p|n}\left(1+\frac{1}{p^s}\right)\sum\limits_{p|n}\ln\left(1+\frac{1}{p^s}\right)}{\prod\limits_{p|n}\left(1+\frac{1}{p^s}\right)}, \tag{3.10}$$

then it suffices to verify that the numerator of (3.10) is positive. Let q be a prime divisor of n. Since

$$\left(1-\frac{1}{x}\right)^{1-\frac{1}{x}}\left(1+\frac{1}{x}\right)^{1+\frac{1}{x}} > 1$$

for all $x > 1$, it follows for $x = q^s$ that

$$\left(1-\frac{1}{q^s}\right)\ln\left(1-\frac{1}{q^s}\right) + \left(1+\frac{1}{q^s}\right)\ln\left(1+\frac{1}{q^s}\right) > 0.$$

Therefore,

$$\begin{aligned}
&\prod_{p|n}\left(1-\frac{1}{p^s}\right)\ln\left(1-\frac{1}{q^s}\right)+\prod_{p|n}\left(1+\frac{1}{p^s}\right)\ln\left(1+\frac{1}{q^s}\right)\\
=\;&\prod_{\substack{p|n\\p\neq q}}\left(1-\tfrac{1}{p^s}\right)\left(1-\tfrac{1}{q^s}\right)\ln\left(1-\tfrac{1}{p^s}\right)+\prod_{\substack{p|n\\p\neq q}}\left(1+\tfrac{1}{p^s}\right)\left(1+\tfrac{1}{q^s}\right)\ln\left(1+\tfrac{1}{q^s}\right)\\
>\;&\prod_{\substack{p|n\\p\neq q}}\left(1-\frac{1}{p^s}\right)\left\{\left(1-\frac{1}{q^s}\right)\ln\left(1-\frac{1}{q^s}\right)+\left(1+\frac{1}{q^s}\right)\ln\left(1+\frac{1}{q^s}\right)\right\}\\
>\;&0.
\end{aligned}$$

Hence

$$\begin{aligned}
&\prod_{p|n}\left(1-\frac{1}{p^s}\right)\sum_{p|n}\ln\left(1-\frac{1}{p^s}\right)+\prod_{p|n}\left(1+\frac{1}{p^s}\right)\sum_{p|n}\ln\left(1+\frac{1}{p^s}\right)\\
=\;&\sum_{q|n}\left\{\prod_{p|n}\left(1-\frac{1}{p^s}\right)\ln\left(1-\frac{1}{q^s}\right)+\prod_{p|n}\left(1+\frac{1}{p^s}\right)\ln\left(1+\frac{1}{q^s}\right)\right\}\\
>\;&0.
\end{aligned}$$

This proves that $\beta_s(n)>0$. Thus by (3.9), we have the inequality (3.8).

Finally, since k is unlimited, then by Theorem 2.3 we get

$$\omega_n=\prod_{i=1}^{k}\frac{p_i}{p_i-1}\simeq+\infty. \tag{3.11}$$

It follows from (3.7) that

$$\alpha_s(n)>2\prod_{i=1}^{k}\frac{p_i^{2s}}{p_i^{2s}-1}=2\omega_n\pounds_n, \tag{3.12}$$

where

$$\pounds_n=\prod_{i=1}^{k}\frac{p_i^{2s-1}}{p_i^{2s-1}+p_i^{2s-2}+...+p_i+1}\leq 1.$$

Moreover, we see that

$$\begin{aligned}
\pounds_n &= \underbrace{\prod_{i=1}^{k}\frac{p_i}{p_i-1}...\prod_{i=1}^{k}\frac{p_i}{p_i-1}}_{(2s-1)\text{-times}}\prod_{i=1}^{k}\frac{(p_i-1)^{2s-1}}{p_i^{2s-1}+p_i^{2s-2}+...+p_i+1}\\
&\geq \omega_n^{2s-1}\phi_n, \qquad (3.13)
\end{aligned}$$

where

$$\phi_n=\prod_{i=1}^{k}\frac{(p_i-1)^{2s-1}}{p_i^{2s-1}+p_i^{2s-2}+...+p_i+1}.$$

Since $\pounds_n$ is limited and $\omega_n\simeq+\infty$, then $\phi_n\leq\frac{\pounds_n}{\omega_n^{2s-1}}\simeq 0$. Thus, we complete the proof of Theorem 3.7 by combining (3.8), (3.12) and (3.13). □

Based on the Remark 2.1 and as a complement to the result of Theorem 2.2, we provide a similar study using the set W_∞, which is external (see the proof of Lemma 3.1).

Theorem 3.8. *If s is limited, then there are infinitely many $n \in W_\infty$ such that*

$$\frac{\varphi_s(n)\,\psi_s(n)}{n^{2s}} < 1 - \oslash, \tag{3.14}$$

where $\oslash$ is an infinitesimal real number independent of n.

Proof. Let r be an unlimited positive integer with $r \geq 2$. We put $a_r = \dfrac{p_{r-1}}{p_r}$ and $d_{r-1} = p_r - p_{r-1}$, where p_r is the r-th prime number. Define

$$\Delta_{r,s} = \left\{ n \in \mathbb{N}\,;\, \frac{\varphi_s(n)\,\psi_s(n)}{n^{2s}} > a_r \right\}.$$

It is clear that $\Delta_{r,s} \neq \emptyset$ because it contains infinitely many prime powers. For example, for every $p > \left(\dfrac{p_r}{d_{r-1}}\right)^{\frac{1}{2s}}$, we have $p, p^2 \in \Delta_{r,s}$. Further, for every $n \in \mathbb{N}^\sigma$, we have $n \notin \Delta_{r,s}$.

First, we verify that if $n \notin \Delta_{r,s}$, then $mn \notin \Delta_{r,s}$ for every $m \geq 1$. In fact, let m, n be two positive integers such that $mn \in \Delta_{r,s}$. Since

$$a_r < \frac{\varphi_s(mn)\,\psi_s(mn)}{(mn)^{2s}} = \prod_{p|mn} \frac{p^{2s}-1}{p^{2s}} \leq \prod_{p|n} \frac{p^{2s}-1}{p^{2s}} = \frac{\varphi_s(n)\,\psi_s(n)}{n^{2s}},$$

it follows that $n \in \Delta_{r,s}$. As required.

Second, from the Prime Number Theorem and since s is limited we obtain

$$\left(\frac{p_r}{d_{r-1}}\right)^{\frac{1}{2s}} \simeq +\infty.$$

Thus, for every limited prime p we get

$$\left(\frac{p_r}{d_{r-1}}\right)^{\frac{1}{2s}} > p. \tag{3.15}$$

It follows from Cauchy's principle that (3.15) holds for some unlimited prime p_m, and therefore $p_m \notin \Delta_{r,s}$. Hence, for every $w \in W_\infty$ we have

$$\frac{\varphi_s(wp_m)\,\psi_s(wp_m)}{(wp_m)^{2s}} \leq a_r,$$

because $wp_m \notin \Delta_{r,s}$. Moreover, it follows from the definition of φ_s and ψ_s that

$$\frac{\varphi_s(wp_m)\,\psi_s(wp_m)}{(wp_m)^{2s}} \neq a_r,$$

since p_{r-1} and wp_m are odd. Thus, (3.14) holds for infinitely many positive integers $n \in W_\infty$, where $\oslash = 1 - a_r \simeq 0$. □

Remark 3.2. In the case when $\oslash$ and s satisfy the hypothesis of Theorem 3.8, then from the Prime Number Theorem and Theorem 2.3 we can prove that

$$\frac{\varphi_s(n)\,\psi_s(n)}{n^{2s}} < a_r \tag{3.16}$$

holds for some $n \in W_\infty$, and therefore we have infinitely many others. In fact, assume that $\dfrac{\varphi_s(n)\,\psi_s(n)}{n^{2s}} \geq a_r$ for any $n \in W_\infty$. Using (2.4), there exists an unlimited prime number p_m such that

$$p_m < \left(1 + \frac{p_{r-1}-1}{d_{r-1}+1}\right)^{\frac{1}{2s}} \simeq +\infty. \tag{3.17}$$

Moreover, we can easily choose an unlimited positive integer i_0 such that

$$p_{m-i_0}p_{m-i_0+1}\dots p_{m-1}p_m = n \in W_\infty.$$

For example $i_0 = \left[\dfrac{m}{2}\right]$, where $[x]$ represents the biggest integer less than or equal to x. It follows from the hypothesis and (3.17) that

$$\frac{1}{a_r} \geq \frac{n^{2s}}{\varphi_s(n)\,\psi_s(n)} = \prod_{p|n}\frac{p^{2s}}{p^{2s}-1} \geq \frac{p_m^{2s}}{p_m^{2s}-1} > \frac{p_r}{p_{r-1}-1}.$$

That is, $p_{r-1} < p_{r-1} - 1$, which is a contradiction.

Finally, let $n_0 \in W_\infty$ such that (3.16) holds. It is also clear that n_0^i satisfies (3.16) for every $i \geq 1$.

Remark 3.3. Let m be a positive integer with $m \geq 2$ and let A be an arbitrary infinite subset of positive integers. We can prove that there are infinitely many $n \in A$ such that

$$(\varphi(n)\,\tau(n))^m > \varphi(n^m)\,\tau(n^m). \tag{3.18}$$

Indeed, since $n \mapsto \varphi(n)\,\tau(n)$ is multiplicative, it is easily seen that there are infinitely many arbitrary prime powers satisfying (3.18).

Some nonclassical notes on the inequality (3.18) are given as follows.

Proposition 3.1. *Let m be a positive integer, with $m \geq 2$. There are infinitely many $n \in L_\infty$ such that*

$$\frac{\varphi(n^m)\,\tau(n^m)}{(\varphi(n)\,\tau(n))^m} = \left(\frac{m+1}{2}\right)^{\omega(n)}\phi_n,$$

where ϕ_n is an infinitesimal real number depending only on m and n.

Proof. Let $n = p_1p_2...p_k \in L_\infty$, where $k \simeq +\infty$. By definition, we see that

$$\begin{aligned}\frac{\varphi(n^m)\,\tau(n^m)}{(\varphi(n)\,\tau(n))^m} &= \prod_{i=1}^{k}\left(\frac{p_i}{p_i-1}\right)^{m-1}\left(\frac{m+1}{2^m}\right)^k \\ &= \left(\frac{m+1}{2}\right)^k\prod_{i=1}^{k}\left(\frac{p_i}{2(p_i-1)}\right)^{m-1} \\ &= \left(\frac{m+1}{2}\right)^{\omega(n)}\phi_n.\end{aligned} \tag{3.19}$$

Using (3.11), we get

$$\phi_n = \prod_{i=1}^{k}\left(\frac{p_i}{2(p_i-1)}\right)^{m-1} < \prod_{i=2}^{k}\left(\frac{p_i-1}{p_i}\right)^{m-1} \leq \left(\frac{2}{\omega_n}\right)^{m-1} \simeq 0.$$

Therefore, $\phi_n \simeq 0$. This completes the proof. □

Proposition 3.2. *Let m be a positive integer with $m \geq 2$. If the Dickson's conjecture is true, then there are infinitely many n such that*

$$\frac{\varphi(n^m)\tau(n^m)}{(\varphi(n)\tau(n))^m} \simeq \begin{cases} @, & \text{if } m \text{ is limited} \\ \oslash, & \text{otherwise.} \end{cases}$$

Proof. Let k, q be limited positive integers with $q \geq 2$ and let $L_{q,k}$ be the infinite subset defined in Theorem 2.1. For every unlimited $n \in L_{q,k}$ and for every positive integer l with $2 \leq l \leq q$, we have

$$n + l = lt_1t_2...t_k,$$

where $t_1, t_2, ..., t_k$ are distinct primes. Since k is limited, then we can separate these primes as follows:

1. Assume that $t_i \simeq +\infty$, for $i = 1, 2, ..., k$. Since $(l, t_1t_2...t_k) = 1$, it follows that

$$\begin{aligned} \frac{\varphi((n+l)^m)\tau((n+l)^m)}{(\varphi(n+l)\tau(n+l))^m} &= \frac{\varphi((lt_1t_2...t_k)^m)\tau((lt_1t_2...t_k)^m)}{(\varphi(lt_1t_2...t_k)\tau(lt_1t_2...t_k))^m} \\ &= \frac{\varphi(l^m)\tau(l^m)}{(\varphi(l)\tau(l))^m}\frac{(m+1)^k}{2^{km}}\frac{(t_1t_2...t_k)^{m-1}(t_1-1)(t_2-1)...(t_k-1)}{[(t_1-1)(t_2-1)...(t_k-1)]^m} \\ &\simeq \frac{\varphi(l^m)\tau(l^m)}{(\varphi(l)\tau(l))^m}\frac{(m+1)^k}{2^{km}} \qquad (3.20) \\ &= @, \end{aligned}$$

for m limited. In the case when m is unlimited, assume that $l = q_1^{a_1}q_2^{a_2}...q_r^{a_r}$, where $q_1, q_2, ..., q_r$ are distinct limited primes and $a_1, a_2, ..., a_r$ are limited positive integers. Since $q_1 \geq 2$ and $m \simeq +\infty$, then from (3.19) we obtain

$$\begin{aligned} \frac{\varphi(l^m)\tau(l^m)}{(\varphi(l)\tau(l))^m}\frac{(m+1)^k}{2^{km}} &\simeq \prod_{i=1}^{r}\left(\frac{q_i}{q_i-1}\right)^{m-1}\prod_{i=1}^{r}\frac{ma_i+1}{(a_i+1)^m}\frac{(m+1)^k}{2^{km}} \\ &= \left(\frac{\frac{q_1}{2(q_1-1)}}{a_1+1}\right)^{m-1}\prod_{i=2}^{r}\left(\frac{\frac{q_i}{q_i-1}}{a_i+1}\right)^{m-1}\prod_{i=1}^{r}\frac{ma_i+1}{a_i+1}\frac{(m+1)^k}{2^{km-1}} \qquad (3.21) \\ &\simeq 0. \end{aligned}$$

2. Assume that t_i is standard, for $i = 1, 2, ..., i_0$ and t_i is unlimited, for $i = i_0 + 1, i_0 + 2, ..., k$. In this case, we see that $n + l = lt_1t_2...t_{i_0}t_{i_0+1}...t_k$ and $(lt_1t_2...t_{i_0}, t_{i_0+1}...t_k) = 1$. When m limited or unlimited, replacing the limited l by $lt_1t_2...t_{i_0}$ and k by $(k - i_0)$ in both (3.20) and (3.21), then we get the desired equations. This completes the proof. □

Theorem 3.9. *Let ℓ be a limited positive integer. For every unlimited n, we have*

$$\varphi(n)\tau(n) > n + \omega(n)\ell.$$

Proof. Let q^α be an unlimited prime power, that is, either α or q is unlimited. Since $1 - \frac{1}{q}$ is appreciable, $\alpha + 1 \geq 2$ and $\frac{\ell}{q^\alpha} \simeq 0$, then

$$\left(1 - \frac{1}{q}\right)(\alpha + 1) > 1 + \frac{\ell}{q^\alpha} = 1 + \frac{\omega(q^\alpha)\ell}{q^\alpha}.$$

It follows that

$$\varphi(q^\alpha)\tau(q^\alpha) > q^\alpha + \omega(q^\alpha)\ell. \tag{3.22}$$

On the other hand, let p^β be an arbitrary prime power with $\beta \geq 1$. Since $\left(1-\frac{1}{p}\right)(\beta+1) \geq 1$, then

$$\varphi\left(p^\beta\right)\tau\left(p^\beta\right) \geq p^\beta. \tag{3.23}$$

Thus, (3.22) is true for every unlimited n which has only unlimited prime powers and (3.23) is true for every $n \geq 1$ because φ and τ are multiplicative.

Now, let n be an unlimited positive integer. There are two cases.

I. Assume that $n = ab$, where $(a,b) = 1$, a is limited, b is unlimited and has only unlimited prime powers. Then

$$\varphi(n)\tau(n) = \varphi(a)\tau(a)\varphi(b)\tau(b) \geq a\varphi(b)\tau(b) > a(b+\omega(b)\ell). \tag{3.24}$$

It suffices to prove that $a\omega(b) \geq \omega(ab)$. In fact, for $a = 1$ the inequality is obvious. In the case when $a \geq 2$, there are two cases to consider.

1. If $\omega(b) \geq 2$, since $a > \omega(a)$ and $(a,b) = 1$, then

$$\begin{aligned} a\omega(b) - \omega(ab) &= a\omega(b) - \omega(a) - \omega(b) \\ &= \omega(b)(a-1) - \omega(a) \\ &\geq \omega(b)\omega(a) - \omega(a) \\ &= \omega(a)(\omega(b)-1) \\ &\geq 1. \end{aligned}$$

2. If $\omega(b) = 1$, then

$$\omega(ab) = \omega(a) + \omega(b) = \omega(a) + 1 \leq a = a\omega(b).$$

Therefore, by (3.24), we obtain

$$\varphi(n)\tau(n) > ab + \omega(ab)\ell = n + \omega(n)\ell.$$

II. Assume that n can not be written as the product of two positive integers a and b, where $(a,b) = 1$, a is limited and b is unlimited which has only unlimited prime powers. Therefore, we must have

$$n = q_1^{\alpha_1} q_2^{\alpha_2} ... q_k^{\alpha_k} \text{ with } k \simeq +\infty,$$

where $q_1^{\alpha_1} < q_2^{\alpha_2} < ... < q_k^{\alpha_k}$ and for every standard j, $q_j^{\alpha_j}$ is standard. In this case, the following set

$$T = \left\{ t \in \mathbb{N}^* ; \varphi\left(\prod_{i=1}^{t} q_i^{\alpha_i} \times q_k^{\alpha_k}\right) \tau\left(\prod_{i=1}^{t} q_i^{\alpha_i} \times q_k^{\alpha_k}\right) > \prod_{i=1}^{t} q_i^{\alpha_i} \times q_k^{\alpha_k} + \omega\left(\prod_{i=1}^{t} q_i^{\alpha_i} \times q_k^{\alpha_k}\right)\ell \right\}$$

is a prehalo and containing the galaxy $\mathbb{N}^\sigma$. That is for every $t \in \mathbb{N}^\sigma$, $t \in T$ (here, we have used the previous part, i.e., the inequality $\varphi(n)\tau(n) > n + \omega(n)\ell$ holds for every n of the form ab, where $(a,b) = 1$, a is limited, b is unlimited and has only unlimited prime powers). Thus, T contains $\mathbb{N}^\sigma$ strictly according to Cauchy's principle because it is internal. Let $w \in T$ be an unlimited with $w < k$. For $n_1 = q_1^{\alpha_1} q_2^{\alpha_2} ... q_w^{\alpha_w} \times q_k^{\alpha_k}$, we get

$$\varphi(n_1)\tau(n_1) > n_1 + \omega(n_1)\ell. \tag{3.25}$$

Moreover, for $n_2 = q_{w+1}^{\alpha_{w+1}} q_{w+2}^{\alpha_{w+2}} ... q_{k-1}^{\alpha_{k-1}}$ we get

$$\varphi(n_2)\tau(n_2) > n_2 + \omega(n_2)\ell, \tag{3.26}$$

because n_2 has only unlimited prime factors (also, we have used the previous part, i.e., the inequality $\varphi(n)\tau(n) > n + \omega(n)\ell$ holds for every n which has unlimited prime powers). Finally by (3.25), (3.26) and since $(n_1, n_2) = 1$, we obtain

$$\begin{aligned}\varphi(n)\tau(n) &= \varphi(n_1 n_2) = \varphi(n_1)\tau(n_1)\varphi(n_2)\tau(n_2) > (n_1 + \omega(n_1)\ell)(n_2 + \omega(n_2)\ell) \\ &> n_1 n_2 + \omega(n_1 n_2)\ell = n + \omega(n)\ell.\end{aligned}$$

This completes the proof of Theorem 3.9. □

Corollary 3.1. *Let $s \geq 1$. For every unlimited n, we have*

$$\frac{\varphi_s(n)\tau(n)}{n^s} > 1 + \phi_n,$$

where ϕ_n is certain positive constant depending only on n with $\phi_n \simeq 0$.

Proof. Let n be unlimited. From Theorem 3.9, we have

$$\varphi_s(n)\tau(n) > n^s + \omega(n)\ell,$$

which can be shown by induction on s. Thus, we may immediately get the assertion since $\dfrac{\omega(n)\ell}{n} \simeq 0$. □

Proposition 3.3. *Let ℓ be a limited positive integer. For every unlimited n, we have*

$$\frac{\varphi(n)\tau(n)}{\omega(n)(n+\ell)} \simeq \begin{cases} @, \text{ if } \tau(n) \text{ is limited} \\ +\infty, \text{ otherwise.} \end{cases}$$

Proof. Let $n = q_1^{\alpha_1} q_2^{\alpha_2} ... q_{\omega(n)}^{\alpha_{\omega(n)}}$ be an unlimited positive integer, where q_i are distinct primes and $\alpha_i \geq 1$, for $i = 1, 2, ..., \omega(n)$. We distinguish two cases:

I. Assume that $\tau(n)$ is limited, then $\omega(n)$ can not be unlimited. Thus,

$$\frac{\varphi(n)\tau(n)}{\omega(n)(n+\ell)} = @\frac{\varphi(n)}{n+\ell},$$

where $@ = \dfrac{\tau(n)}{\omega(n)}$. Moreover, we see that

$$\frac{\varphi(n)}{n+\ell} \simeq \frac{\varphi(n)}{n} = \prod_{i=1}^{\omega(n)} \frac{q_i - 1}{q_i} = @, \tag{3.27}$$

which we may because $\omega(n)$ is limited.

II. Assume that $\tau(n)$ is unlimited. In this case, we also distinguish two cases:

II.1. If $\omega(n)$ is limited, then by (3.27) we have

$$\frac{\varphi(n)\tau(n)}{\omega(n)(n+\ell)} = @\frac{\varphi(n)}{n+\ell}\tau(n) \simeq +\infty,$$

where $@ = \dfrac{1}{\omega(n)}$.

II.2. If $\omega(n)$ is unlimited, it follows from (3.27) that

$$\begin{aligned}
\frac{\varphi(n)\tau(n)}{\omega(n)(n+\ell)} &\geq \frac{\varphi(n)}{n+\ell}\frac{2^{\omega(n)}}{\omega(n)} \\
&\simeq \prod_{i=1}^{\omega(n)}\frac{q_i-1}{q_i}\frac{2^{\omega(n)}}{\omega(n)} \\
&= \frac{\prod_{i=1}^{\omega(n)}\frac{2q_i-2}{q_i}}{\omega(n)} \\
&> \frac{\left(1+\frac{1}{3}\right)^{\omega(n)-1}}{\omega(n)} \qquad (3.28) \\
&\simeq +\infty,
\end{aligned}$$

where (3.28) holds because

$$1 \leq \frac{2q_1-2}{q_1} < \frac{2q_2-2}{q_2} < ... < \frac{2q_{k-1}-2}{q_{k-1}} \simeq \frac{2q_k-2}{q_k} \simeq 2,$$

and $\frac{2q_2-2}{q_2} \geq \frac{4}{3}$. Therefore, $\frac{\varphi(n)\tau(n)}{\omega(n)(n+\ell)} \simeq +\infty$. This completes the proof of Proposition 3.3. □

Remark 3.4. The previous two external subsets $\oslash$ and $\pounds$ are also considered to be additive convex subgroups of $\mathbb{R}$ (denoted by N and called neutrices [11]). Moreover, we see that $\oslash + \pounds = \pounds$, $\pounds.\pounds = \pounds$, $\pounds.\oslash = \oslash$ and $\pounds = 1 + \pounds = 2 + \pounds$. In this subject, there are several additive convex subgroups of $\mathbb{R}$ involving $\oslash$ and $\pounds$. For details, see [11]. An important point of the above notions that the sum of two neutrices M and N is equal to $\max(M, N)$, see [9].

We finish this paper by the following two results which give a relationship between multiplicative functions and external subsets.

Lemma 3.2. *Let $f : \mathbb{N} \longrightarrow \mathbb{N}$ be a standard multiplicative function and let N be an additive convex subgroup of $\mathbb{R}$. The flexible arithmetic function*

$$\begin{aligned}
\Psi_{f,N} &: \mathbb{N}^{\sigma} \longrightarrow \mathbb{R} \\
n &\longmapsto f(n) + N
\end{aligned}$$

is multiplicative if and only if $N^2 \subseteq N$.

Proof. Let $n_1, n_2 \in \mathbb{N}^{\sigma}$ such that $(n_1, n_2) = 1$. Assume that $N^2 \subseteq N$. Then by [11, p. 145-170] we have

$$\begin{aligned}
\Psi_{f,N}(n_1 n_2) &= f(n_1 n_2) + N \\
&= f(n_1) f(n_2) + \max\left(f(n_1) N, f(n_2) N, N^2\right) \\
&= f(n_1) f(n_2) + f(n_1) N + f(n_2) N + N^2 \\
&= (f(n_1) + N)(f(n_2) + N) \\
&= \Psi_{f,N}(n_1)\Psi_{f,N}(n_2),
\end{aligned}$$

which we may because $N+N^2=\max\left(N,N^2\right)=N$, $f\left(n_1\right)$ and $f\left(n_2\right)$ are standard and therefore $f\left(n_1\right)N=f\left(n_2\right)N=N$. Thus, $\Psi_{f,N}$ is multiplicative.

Conversely, assume that $\Psi_{f,N}$ is multiplicative. We see that

$$\begin{aligned}\Psi_{f,N}\left(n_1n_2\right) &= f\left(n_1n_2\right)+N\\ &= \left(f\left(n_1\right)+N\right)\left(f\left(n_2\right)+N\right)\\ &= f\left(n_1n_2\right)+N+N^2.\end{aligned}$$

It follows that $N+N^2=N\left(1+N\right)=N$. We distinguish two cases.

1. If $1\notin N$, then for any $x\in N$ we have x is not appreciable, otherwise $1=\dfrac{x}{x}\in\dfrac{N}{x}=N$ which contradicts the fact that $1\notin N$. Moreover, since we can not find an additive convex subgroup of $\mathbb{R}$ between $\oslash$ and $\pounds$, then $N\subseteq\oslash$, and so $N^2\subseteq N$.

2. If $1\in N$, then $1+N=N$ because N is convex. Therefore, $N^2=N$. □

Proposition 3.4. *Let M,N be two additive convex subgroups of $\mathbb{R}$ such that $M\subset N$, $N^2\subseteq N$ and $1\notin M$ (for example, $\oslash\subset\pounds$, $\pounds^2\subseteq\pounds$ and $1\notin\oslash$) and let f and g be two standard multiplicative functions with $g\neq 0$, then*

$$n\in\mathbb{N}^\sigma\mapsto\frac{f\left(n\right)+N}{g\left(n\right)+M}$$

is multiplicative.

Proof. Let $n\in\mathbb{N}^\sigma$. We see that

$$\frac{f\left(n\right)+N}{g\left(n\right)+M}=\frac{f\left(n\right)}{g\left(n\right)}\left(\frac{1+N}{1+M}\right). \tag{3.29}$$

On the other hand, since $1\notin M$ then from the proof of Lemma 3.2 we have $M\subseteq\oslash$. Since for every $\phi\in M$,

$$\frac{1}{1+\dfrac{-\phi}{1+\phi}}=1+\phi,$$

where $\dfrac{-\phi}{1+\phi}\in M$ because it is a convex subgroup, we obtain

$$\frac{1}{1+M}=1+M. \tag{3.30}$$

It follows from (3.29) and (3.30) that

$$\begin{aligned}\frac{f\left(n\right)+N}{g\left(n\right)+M} &= \frac{f\left(n\right)}{g\left(n\right)}\left(1+M\right)\left(1+N\right)\\ &= \frac{f\left(n\right)}{g\left(n\right)}+\max\left(M,N,MN\right)\\ &= \frac{f\left(n\right)}{g\left(n\right)}+N,\end{aligned}$$

because $M\subset N$. Hence by Lemma 3.2, we get the result since $\dfrac{f}{g}$ is multiplicative and $N^2\subseteq N$. □

Acknowledgements. The author would like to thank professor Boris Hasselblatt for his suggestions to make this paper.

REFERENCES

[1] Dj. Bellaouar, A. Boudaoud and Ö. Özer. *On a sequence formed by iterating a divisor operator*. Czech. Math. J. *Accepted*.

[2] Dj. Bellaouar and A. Boudaoud, *Nonclassical study on the simultaneous rational approximation*, Malays.J. Math. Sci. **9**, No. 2 (2015), 209-225.

[3] Dj. Bellaouar, *Notes on certain arithmetic inequalities involving two consecutive primes*. Malays.J. Math. Sci. **10**, No. 3 (2016), 263-278.

[4] A. Boudaoud, La conjecture de Dickson et classes particulière d'entiers, *Ann. Math. Blaise Pascal*. **13** (2006), 103-109.

[5] A. Boudaoud, Decomposition of terms in Lucas sequences, *J. Log. Anal.* **1** (2009), 1-23.

[6] J.M. De Koninck and A. Mercier, *1001 problèmes en théorie classique des nombres*, Ellipses Edition Marketing S.A, Paris, 2004.

[7] F. Diener and M. Diener, *Nonstandard analysis in practice*, Springer Science & Business Media, 1995.

[8] B. Dinis and I.P. Van Den Berg, Algebraic properties of external numbers, *J. Log. Anal*. **3** (2011), 1-30.

[9] J. Justino and I.P Ven Den Berg, Cramer's rule applied to flexible systems of linear equations, *Electronic Journal of Linear Algebra*. **24** (2012), 126-152.

[10] T. Krassimir, *Note on φ, ψ and σ-functions. Part 3*, Notes Number Theory Discrete Math., Vol. **17**, 2011, No. 3, 13-14.

[11] F. Koudjeti, I.P. van den Berg, Neutrices, external numbers and external calculus, in: Nonstandard Analysis in Practice, F. and M. Diener (eds.), Springer Universitext (1995) 145-170.

[12] E. Nelson, *Internal set theory*, Bull. Amer. Math. soc. **83** (1977), 1165-1198.

[13] Paulo Ribenboim, The Little Book Of Big Primes, Springer - Verlag, 1991.

[14] A. Robinson, *Non-standard Analysis*, Princeton University Press, 1974.

[15] I.P. Van Den Berg, *Extended use of IST*, Ann. Pure Appl. Logic. **58** (1992), 73-92.

[16] D. Wells, *Prime numbers, the most mysterious figures in math*, John Wiley & Sons, Inc., Canada, 2005.

UNIVERSITY OF GUELMA
DEPARTMENT OF MATHEMATICS
GUELMA, ALGERIA
E-mail address: bellaouar.djamel@univ-guelma.dz

A New Efficient Approach Based on Chaotic Map for Image Encryption

Ali HADOUDA
RIIR Laboratory
Faculty of Exact and Applied Sciences
Université Oran1
BP 1524 El M'Naouer, Oran,Algeria
alihadouda111@gmail.com

Najia TRACHE
RIIR Laboratory
Faculty of Exact and Applied Sciences
Université Oran1
BP 1524 El M'Naouer, Oran,Algeria
n_khelfi@yahoo.fr

Mohamed Fayçal KHELFI
RIIR Laboratory
Faculty of Exact and Applied Sciences
Université Oran1
BP 1524 El M'Naouer, Oran,Algeria
mf_khelfi@yahoo.fr

Abstract—The protection and security of data and information have become of paramount importance in the deferential areas including imaging, so it is best to protect them before transmitting them. Today, various types of techniques and methods based on Chaotic Encryption are used to overcome several types of threats. In this paper, we propose a new efficient image encryption system using a new simple function permutation pixels(confusion) of an image and a chaotic generator map, the proposed cryptosystem based on three steps: confusion, shuffling, diffusion. In the confusion step, the pixels of the original image is swapped by a simple permutation function. In the shuffling step, the confusing image is devised over four blocks as each block of pixels of the image is mixed, allowing to give more unpredictability. In the diffusion step, the shuffling image is diffused by combining chaotic sequence generated from the chaotic generator map used. The evaluation parameters used are: Number of Pixel Rate Changes (NPCR), Unified Average Change Intensity (UACI), Peak Signal to Noise Ratio (PSNR) and Mean Square Error (MSE).

Keywords— image encryption, Chaotic generator, permutation of pixels, NPCR, UACI.

1. Introduction:

The security needs of real life always remain increasing. For this reason, many people have developed cryptographic systems to achieve these needs. When we talk about cryptography several interpretations arise which can be used to achieve the flexibility, compliance, and privacy of data that is a requirement in today's systems. Mathematicians and scientists, starting from Shanon's that date back to 1949 [1] have proposed several cryptographic algorithms up to now like AES, DES, RSA [9,10], ... etc.

All recent work for data security uses Shannon's basic techniques [1][2] that can be classified into two main categories: the transformation of values (confusion) and permutation of positions (diffusion). The combination between them is also possible. Chaos-based encryption algorithms [3] are considered good for practical use as they provide a good combination of high speed, good security, and computational power. Several ways for decreasing effects of Solak's attack or eliminating its possibility were proposed. There are many chaos-based encryption algorithms which introduce the image security in different principle. In [4] A new efficient image cryptosystem based on combination of confusion and diffusion with FRFT to provide the best performance. The proposed algorithm uses Arnold cat map for confusion with the development of a new Henon chaotic map for diffusion in FRFT. In [5] a new method of encryption/decryption based on chaos and confusion-diffusion architecture. They also developed a new algorithm based mostly on two standard chaotic maps, a logistics map, and a sine map. This method is applied for simple and medical images to produce an encrypted image. In [6] they have tried to use a chaotic map to its full potential to build a strong encryption scheme that can withstand any intrusion, and ensure safety of the image. This Image encryption algorithm proposed using mathematical octave tool and verified by the use of a variety of test series.
In [7] a new chaos-based cryptosystem has been proposed for securing images based on Arnold cat map and Henon chaotic map. The Arnold cat map and the Henon map are two discrete chaotic maps that are used in this scheme and the bit shuffling and pixel shuffling are reversible transformations that are performed using the Arnold cat map with various secret parameters. In [8], a new efficient image encryption algorithm using a set of chaotic maps has been proposed, consists of three steps: confusion, shuffling, and diffusion. In confusion step, the original image is confused by using Arnold cat chaotic map. In shuffling step, the pixels of the confused image are shuffled to add more randomness. Finally, the shuffled image is diffused by a key image generated by combining sequences generated from set of Henon chaotic maps.

This paper is organized as follows, the next section describes the main structure of the proposed cryptosystem, and in its subsections, the details of the used cryptosystem components are described. Section 3 presents the security and the influence of the change of the pixels on the clear image by the proposed cryptosystem analysis results.

2. The Proposed Scheme:

The proposed encryption in (Fig.2) shows the block diagram of our proposed encryption which consists of three steps.

In the first step, the image pixels of size N*N is confused based on our simple function of permutation developed. In the pixel permutation, the pixels are shuffled without any alteration in value and histogram. Therefore, the initial conditions and control parameters of this function serve as the first secret key (number iterations of permutation on the image pixels). Our new function used is a simple function to swap the pixels (x,y) of the original image in a new pixel location (x',y') in the permuted image as follow:

For each pixel (x,y) :

x'=x+y, y'=x'+x and b(x',y')= a(y,x) where b(x',y') is the new pixels location in the shuffled image b, a(x,y) is the pixels location of the original image a .

In the second step [8] the confused image is devised over four blocks, each block of pixels of the confused image is mixed as follow (fig.1):

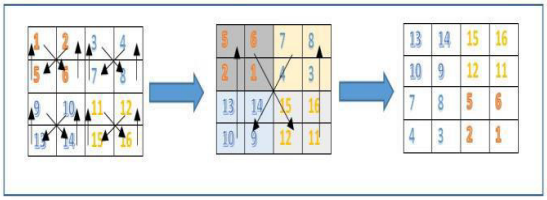


Fig. 1 Pixel shuffling[8].

Step 1: Divide the image into 4 blocks.

Step 2: Each block is shuffled in a predefined order (e.g. the block (1,2,5,6) is shuffled.

Step 3: Step 2 is repeated until it reaches the last quad.

Step 4: Each entire quad is considered as a single cell and shuffled in a predefined order (e.g entire quad (5,6,2,1)) is shuffled to be (13,14,10,9) as shown in fig.2

we have divide the step three into two parts:

1- we adopt a henon chaotic map to generate encryption key images and change the pixel values of the image.

The developed Henon chaotic map is obtained by the equation (1)[4]:

$$x_{i+1} = (r \times x_i + y_i) \bmod 1$$
$$y_{i+1} = x_i - b, \qquad i=0,1,2,\ldots \qquad (1)$$

Where b=0.3, r [0, ∞].The parameter r, the parameter b, initial value x_0 and the initial value x_1 may represent the second key, and the parameters are selected as b=0.3, r=1.4,x_0 =0.02,x_1 =0.08.

2- the shuffling image is X-ORed with the encryption key image.

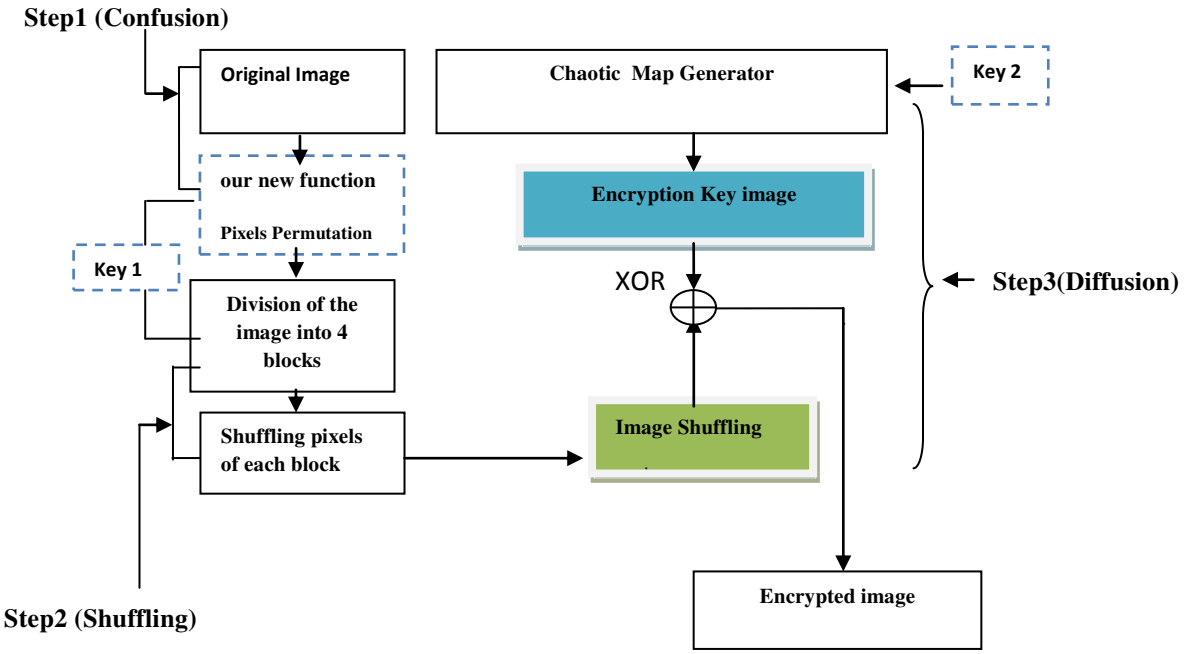


Fig. 2 Our proposed cryptosystem.

3. SECURITY ANALYSIS:

A cryptosystem is said to be reliable if one has the possibility of resisting attacks from intruders, interceptors or any other form of enemies. In this article, we will evaluate the security of crypto by several families of cryptoanalytic:

A- NPCR and UACI Analysis:

NPCR means the change rate of the number of pixels of the cipher image when only one pixel of the plain image is modified. the unified average changing intensity, (UACI) measures the average intensity of differences between the plain

image and ciphered image, The NPCR and UACI of these two images are defined in equations (4), (5) [11,12]:

$$NPCR = \frac{\sum_{i,j} D(i,j)}{W \times H} \times 100\ \% \quad (2)$$

$$UACI = \frac{1}{W \times H}\left[\sum_{i,j} \frac{|C_1(i,j) - C_2(i,j)|}{255}\right] \times 100\ \% \quad (3)$$

Where $D(i,j)$ is defined as

$$D(i,j) = \begin{cases} 0, & if\ (C_1(i,j) = C_2(i,j)) \\ 1, & if\ (C_1(i,j) \neq C_2(i,j)) \end{cases}$$

W and H are the width and height of encrypted image, $C_1(i,j)$ and $C_2(i,j)$ are the pixel's value of the original and the encrypted image respectively.

B-Histogram:

To prevent the access of information to attackers, it is important to ensure that encrypted and original images do not have any statistical similarities. The histogram analysis clarifies how the pixel values of image are distributed. We test the histogram analysis of the proposed encryption algorithm using five plain images as shown in Fig.3 [15].

4- ANALYSIS & QUALITY PERFORMANCE MEASURES:

-PSNR and MSE Analysis[13,14]**:**

A-Peak Signal to Noise Ratio (PSNR):

PSNR is the ratio between the most feasible power of a signal and the power of damage noise that change the reliability of its representation. Because many signals have an extremely wide dynamic range, PSNR is usually specified in terms of the logarithmic decibel (dB) scale. The PSNR can be computed as follows:

$$\text{PSNR} = 10 \times \log_{10} \frac{255 \times 255}{\frac{1}{\text{H} \times \text{W}} \sum_{\text{X}=0}^{\text{H}-1} \sum_{\text{y}=0}^{\text{W}-1} [\text{f(x,y)} - \text{g(x,y)}]^2} \quad (4)$$

where H and W area part of the height and widthof the image, severally; and f(x,y) and g(x,y) area section the graylevels situated at coordinate (x,y) of the first image and attacked image, respectively.

B. Mean Square Error(MSE):

It is considered as an average squared difference between the original image and distorted image. It is calculated by the formula given below:

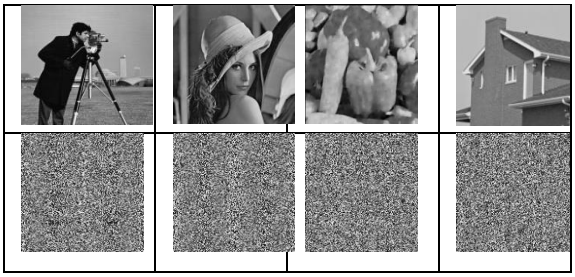
$$MSE = \frac{1}{n}\sum_{i=1}^{n}(\hat{Y}_i - Y_i)^2 \quad (5)$$

where, $\hat{Y}_i$is the distorted image and the Y is the original image[14].

4-EXPERIMENTAL RESULTS:

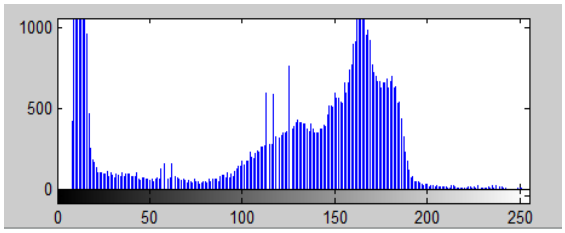
The proposed algorithm uses only one round for confusion, pixel shuffling and diffusion.

All the simulation experiments have been carried out using MATLAB R2014a on Core i3, 4 GB RAM PC. The number of shuffled blocks in the shuffling stage is 64, and the number iterations of permutation on the image pixels =5, The following experiment used four images (Lena, Cameraman, Pepper, and House). These images encrypted with their resolution 256*256.

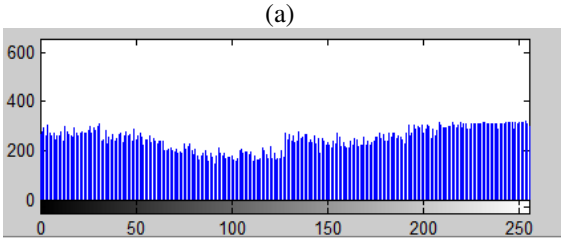


a. Cameraman b.Lena c. Pepper d.House

Fig 3. Original and Encrypted Images.



(a)



(b)

Fig 4. Histogram Analysis ((a)original image, (b)the encrypted image)

image	NPCR (**Our**)	UACI (**Our**)	NPCR **Ref.[6]**	UACI **Ref.[6]**
Cameraman	99,64%	32,11%	99.30	33.65
Lena	99,62%	31,29%	99.61	33.50
Pepper	99,65%	31,20%	99.56	33.46
House	99,63%	28,97%	99.58	33.48

TABLE 1. NPCR and UACI ANALYSIS

image	PSNR (db)	MSE
Cameraman	35.47	2.8347×10^{-4}
Lena	31.83	6.5482×10^{-4}
Pepper	32.49	$2{,}1\times 10^{-3}$
House	31.20	7.5735×10^{-4}

TABLE 2. PSNR and MSE(after encryption)

- (Table 1) shows that the result obtained by our cryptosystem is better than the results found by [6].

5-CONCLUSION AND FUTURE WORK:

In this paper, we have designed and tested an effective new approach based on three steps. The cryptosystem proposed uses a simple function of permutation of the pixels of the image and the characteristics of the high sensitivity of the chaotic systems for the initial values by producing the secret key of the chaotic generator usable in our cryptosystem. The results of the security analysis of four images demonstrate the resistance of our cryptosystem. For our future work, we will use our proposed cryptosystem in this paper in the image watermarking.

REFERENCES

[1] Shannon CE "Communication theory of secrecy system,"Bell System Technical Journal, Volume 28, (1949)pp. 656 – 715.

[2] M.Yang, N. Bourbakis, and S.Li, "Data-image-video encryption," IEEE potentials, (2004), pp. 28-34.

[3] TiegangGao, Zengqiang Chen, "A new image encryption algorithmbased on hyper-chaos", Physics Letters A 372 (2008) pp. 394–400.

[4] Mona F. M. Mursi, HossamEldin H. Ahmed, Fathi E. Abd El-samie, Ayman H. Abd El-aziem "Image Encryption Based on Development of Hénon Chaotic Maps Using Fractional Fourier Transform", Mathematics and Computers in Science and Industry , International Journal of Strategic Information Technology and Applications /ijsita, (2014) pp. 98-106.

[5] M.MADANI, Y.BENTOUTOU, "Cryptage d'images médicales à la base des cartes chaotiques" International Conference Colloque Tassili SCCIBOV.(2015).

[6] BhaskarMondal, Tarni Mandal, "A Nobel Chaos based Secure Image Encryption Algorithm", International Journal of Applied Engineering Research ISSN 0973-4562 Volume 11, Number 5 (2016) pp. 3120-3127.

[7] Ali Soleymani, Md Jan Nordin, and Elankovan Sundararajan, "A Chaotic Cryptosystem for Images Based on Henon and Arnold Cat Map", The Scientific World Journal, Volume 2014, Article ID 536930, 21 pages, (2014).

[8]Hikmat N. Abdullah ,Hamsa A. Abdullah "Image Encryption Using Hybrid Chaotic Map" International Conference on Current Research in Computer Science and Information Technology (ICCIT), Slemani – Iraq (2017).

[9] Prerna Mahajan ,Abhishek Sachdeva "A Study of Encryption Algorithms AES, DES and RSA for Security", Global Journal of Computer Science and Technology Network, Web & Security Volume 13 Issue 15 Version 1.0 (2013).

[10] M. Preetha , M. Nithya "A Study and Performance Analysis Of RSA Algorithm", International Journal of Computer Science and Mobile Computing /IJCSMC, Vol. 2, Issue. 6, June (2013), pp.126 – 139.

[11] Kwok, H.S.; Tang, W.K.S.: "A fast image encryption system based on chaotic maps with finite Precision representation". Chaos Solitons Fractals 32(4), (2007), pp.1518–1529.

[12] Borujeni, S.E, Eshghi,M.: "Chaotic image encryption design using tompkins-paige algorithm", Hindawi Publishing Corporation Mathematical Problem in Engineering vol. 200, (2009), pp. 22 .

[13]M.Hariharalakshmi,M.Sivajothi,M.MohamedSathik, " Survey of Digital Watermarkingtechniques for Data security", International Journal of Innovative Research in Computer and Communication Engineering ,Vol. 5, Issue 3, (2017).

[14]Gursharanjeet Singh Kalra, Rajneesh Talwar, Harsh Sadawarti, "Comparative Analysis of Blind Digital Image Watermarking Utilising Dual Encryption Technique in Frequency Domains", World Journal of Computer Application and Technology (wjcat), DOI:1013189, (2013).

[15] M.A. Mohamed, H.M. Abdel-Atty A.M Aboutaleb, M.G. Abdel-Fattah, A.S. Samrah, "Hybrid Watermarking Scheme for Copyright Protection using Chaotic Maps Cryptography", International Journal of Computer Applications (0975 – 8887) Volume 126 – No.4, (2015).

DNA Encryption Algorithm Based on Variable Coding Scheme

Mustapha MEFTAH
University of Science and Technology Mohamed Boudiaf ORAN
Coding and Information Security Laboratory
Oran, Algieria
meftah_m@hotmail.com

Pr. Adda ALI PACHA
University of Science and Technology Mohamed Boudiaf ORAN
Coding and Information Security Laboratory
Oran, Algeria
a.alipacha@gmail.com

Pr. Naïma HADJ-SAID
University of Science and Technology Mohamed Boudiaf ORAN
Coding and Information Security Laboratory
Oran, Algeria
naima.hadjsaid@univ-usto.dz

Abstract

The basic idea behind the proposed research work is to exploit the robustness of the genetic material in order to improve and outperform the performance of other conventional algorithm.

In this paper, a new symmetric encryption algorithm inspired from DNA is proposed. It is based on a nucleotide base coding method that is not unique.

First, the algorithm codifies the secondary DNA key which is extracted from the main DNA key according to the number of nucleotide base occurrences. The order of the number of appearance of the nucleotide bases defines the coding scheme of each base. Then an XOR operation is applied between the coded DNA sequence and the plaintext. Finally, in order to reinforce our algorithm, we confuse the obtained result using a permutation box.

KEY WORDS: DNA, cryptography, encryption, decryption, algorithm, data security.

I. INTRODUCTION

Generally, the security of traditional cryptography is based on mathematical problems that are difficult to solve. Both the secret key and public key cryptography methods have weaknesses. The keys used are so large that a multitude of powerful computers working at the same time each with about a billion calculations per second would take years to decipher the key. Even through it is not a problem right now, but it will be soon, given the growth in computing power and technology.

A new data security technique has been introduced using the biological structure of DNA called DNA Computing. It was invented by Leonard Max Adleman in 1994, to solve complex problems such as the Hamilton Road problem, the NP-complete problems similar to the problem of the traveling salesman. [1]

DNA can be used to store and transmit data. The concept of using DNA in the fields of cryptography has been identified as a technique that could bring new hope for unbreakable algorithms [2].

In this paper, we propose a symmetric ciphering algorithm based on DNA, it is described in the following, steps.

II. THE PROPOSED ALGORITHM

a. Encryption process

Both parties must previously share a strand secret DNA (The main key) of their choices.

The secondary key is represented by four parameters: Pos_Start, Nbr_Base, an index I and an NR number of round.

Phase 1: Encryption key coding

Let an image M with a length L_M. The coding process of the encryption key:

We will extract a DNA sequence from the Pos_Start position with a Nbr_Base length. Then we calculate the number of occurrences of each nucleotide base A, C, G and T. The result is N_A, N_C, N_G and N_T. We will order the result with ascending order. This order is used to codify the DNA sequence (S) extracted from the index I with a length $L_S = L_M / 2$. The coding of bases in an ascending order is: 00, 01, 10, 11.

With this process, there are 4!=24 coding schemes.

Schemes	A	C	G	T
1	00	01	10	11
2	00	01	11	10
3	00	10	01	11
4	00	10	11	01
5	00	11	01	10
6	00	11	10	01
7	01	00	10	11
8	01	00	11	10
9	01	10	00	11
10	01	10	11	00
11	01	11	00	10
12	01	11	10	00
13	10	00	01	11
14	10	00	11	01
15	10	01	00	11
16	10	01	11	00
17	10	11	00	01
18	10	11	01	00
19	11	00	01	10
20	11	00	10	01
21	11	01	00	10
22	11	01	10	00
23	11	10	00	01
24	11	10	01	00

Tab. 1: The 24 coding schemes

After coding, we will obtain a key sequence S' of length $L_{S'} = 2L_S = L_M$.

The default nucleotide bases order is ACGT. This sequence is used in order of priority to decide in case of an equality of the occurrence number.

Example: For an gray-scale image of size 256 * 256,

L_m=256*256= 65536 $L_S = L_M / 2 = 65536 / 2 = 32768$

N_A=8437 N_C=7951 N_G=5184 N_T=11196

The ascending order of occurrence number is N_T, N_A, N_C, N_G which implies the following coding table:

T	A	C	G
00	01	10	11

Tab. 2: Example of a coding scheme

Phase 2: XOR Operation

In this step, we will proceed to an XOR between the obtained sequence S' and the message M in its binary form which are of the same length $L_{S'} = L_M$. As a result, we will get an encrypted binary sequence C'.

Phase 3: the confusion

The purpose of this step is to scramble the message to improve encryption. We used a permutation box as shown below.

1	2	3	4	5	6	7	8
Odd bits descending							
15	13	11	9	7	5	3	1

9	10	11	12	13	14	15	16
Even bits descending							
16	14	12	10	8	6	4	2

Fig. 1: Permutation box

The encrypted sequence C' is divided into sequences of 16 bits which will each constitute an entry in the permutation box.

The number of rounds is obtained from sub-key NR.

After each round, we will make one right shift.

We will get a ciphered DNA sequence C.

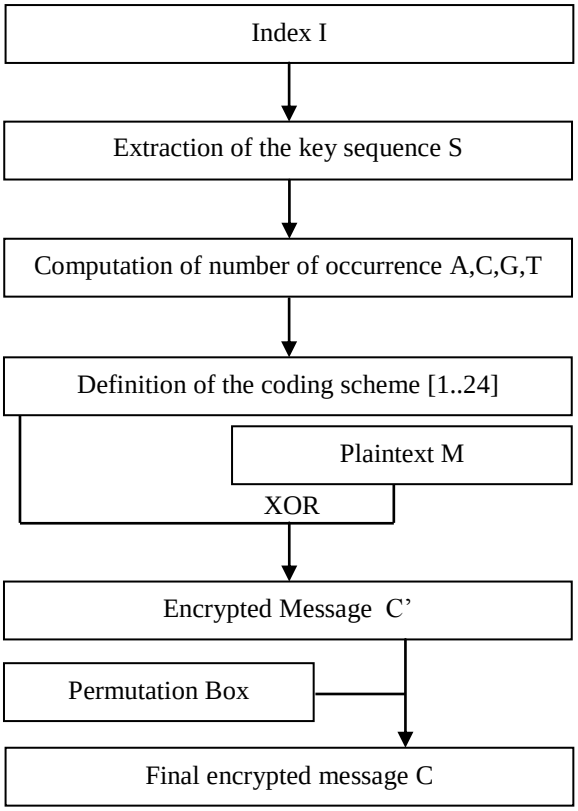


Fig. 2: Diagram of the encryption algorithm

b. Decryption process

Phase 1: Encryption key coding

After receiving the index I and the encrypted message C, we will use this index to extract a DNA sequence S with a length $L_S = L_C / 2$. Then we calculate the number of occurrences of each nucleotide bases A, C, G and T. The result is reported in the variables: N_A, N_C, N_G and N_T. We will order the result in ascending order. This order is used to codify the DNA sequence S. The coding of bases from the smallest to the largest is: 00, 01, 10, 11.

After coding, we will obtain a key sequence S' of length $L_{S'}=L_S*2=L_c$.

Phase 2: Eliminate Confusion

The objective of this step is to eliminate the confusion of the encrypted message. We used a reverse permutation box:

1	2	3	4	5	6	7	8
8	16	7	15	6	14	5	13

9	10	11	12	13	14	15	16
4	12	3	11	2	10	1	9

Fig. 3: Reverse permutation box

The number of rounds is obtained from sub-key NR.

Before each round, we will shift one bit to the left until the end of rounds.

The result obtained is an encrypted message C '

Phase 3: XOR Operation

In this step, we will proceed to an XOR operation between the encrypted message C' and the obtained key sequence S' which have the same length $L_{C'} = L_S$. As a result, we will get the plaintext M.

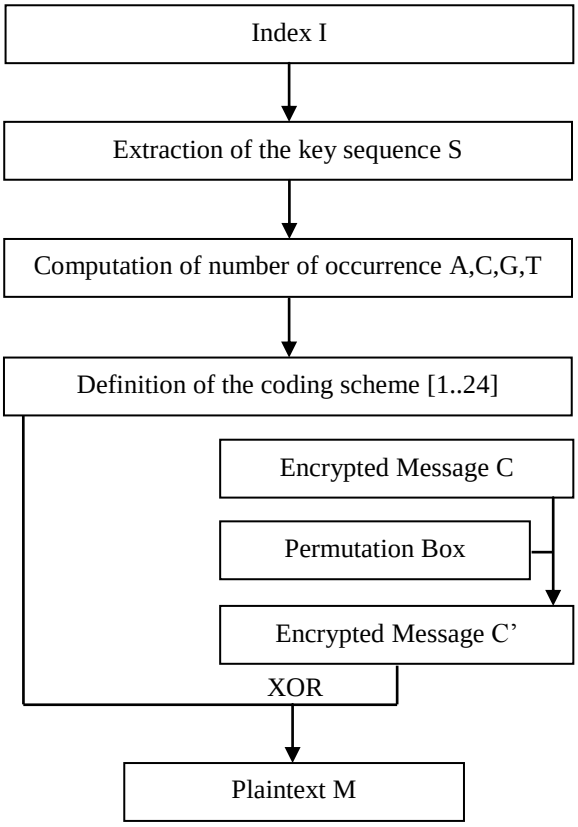


Fig. 4: Diagram of the decryption algorithm

c. Result validation

We have downloaded "Canis lupus familiaris breed boxer chromosome 1" from GenBank https://www.ncbi.nlm.nih.gov/genbank . We use it as main-key.

The main-Key: 122 678 785 nucleotide bases
The sub-key is:

Pos_Start = 100 Nbr_Base = 1000

Index I = 2000 NR (Number of rounds) = 8

The image used is "cameraman.tif" of size 256x256. After implementing the algorithm in "Matlab R2015a", here are the results obtained.

c.1 Test 1: Histogram of Image

For a gray-scale image, the histogram is defined as a discrete function that is associated with each intensity value the number of pixels considering this value. The determination of the histogram is therefore performed by counting the number of pixels for each intensity of the image. The histogram can then be seen as a probability density.

Histograms are resistant to a number of transformations in the image. They are invariant to rotations and translations, as well as to a lesser extent to changes of point of view and changes of scale.

Referring to the results obtained (fig.5 & fig.6), we can clearly see that the sample image differs substantially from the corresponding encrypted one. Moreover, the histogram of the encrypted image is fairly uniform which makes it difficult to extract the pixels for statistical purpose.

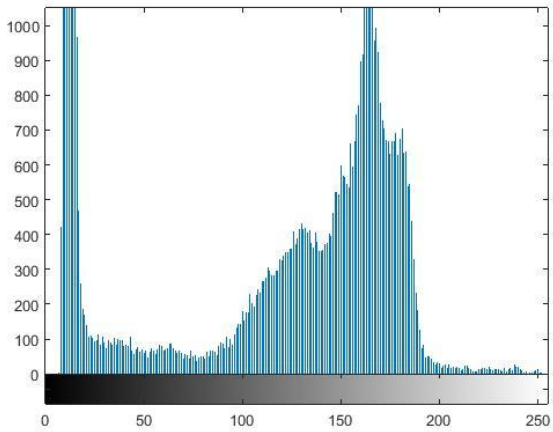


Fig. 5: Plaintext Image « cameraman.tif » And his Histogram

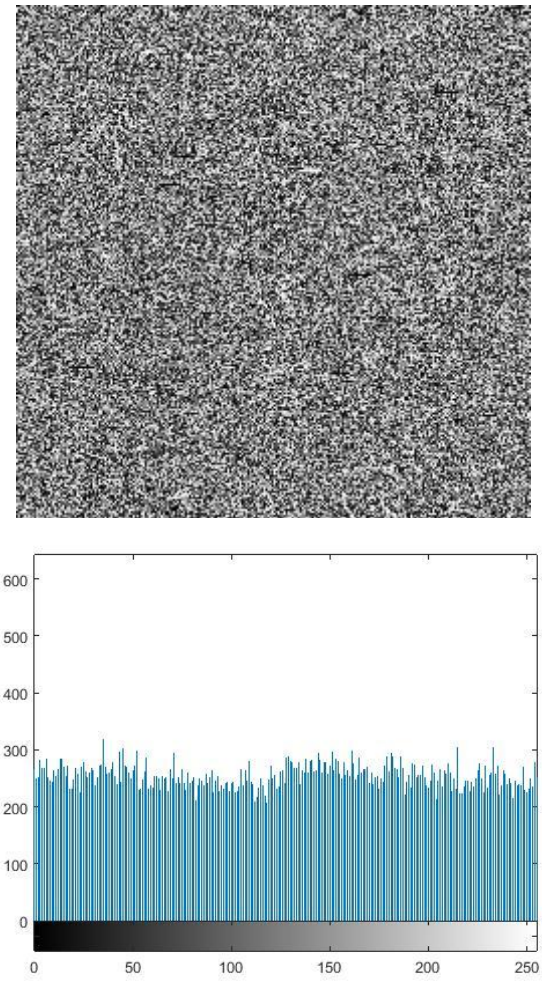


Fig. 6: Ciphered Image « cameraman.tif » and his histogram

c.2 Test 2 : Entropy

Shannon's entropy, due to Claude Shannon, is a mathematical function that intuitively corresponds to the amount of information contained or provided by an information source.

For a source, which is a discrete random variable X with n symbols, each symbol Xi having an occurrence probability Pi, the entropy H of the source X is defined as:

$$H(x) = -\sum_{i=1}^{n} P_i . log_2(P_i) \qquad P_i = \frac{k_i}{n}$$

With i varying from 0 to 255, and n is the number of generated values of the encrypted image (n = 256 * 256 = 65536), ki is the frequency of each number i.

We usually use a logarithm with base 2 because the unit of entropy is bit/symbol. The symbols represent the possible realizations of the random variable X.

Let's take a source consisting of a 256 characters. If these characters have the same probability, the entropy associated with each character is:
$\log_2(256) = \log_2(2^8) = 8$ bits, which means it takes 8 bits to transmit a character.

The ideal is to find the entropy of the encrypted image that is close to a source providing characters having the same probability.

Here is the obtained result: $e_M = 7.0097$ - $e_C = 7.9957$
e_M: The entropy of the plaintext image "cameraman.tif"
e_C: The entropy of the encrypted image:

c3. Test3: Correlation between Adjacent pixels

In probabilities and statistics, studying the correlation between two random variables or numerical statistics is to study the intensity of the connection that can exist between these variables. The link sought is a refined relation, it is the linear regression.

The correlation coefficient is between -1 and 1. The intermediate values provide information on the degree of linear dependence between the two variables. The closer the coefficient is to the extreme values -1 and 1, the stronger the correlation between the variables. A correlation of 0 means that the variables are not correlated.

In our case, we took 2000 pixels randomly and we studied the correlation between adjacent pixels.

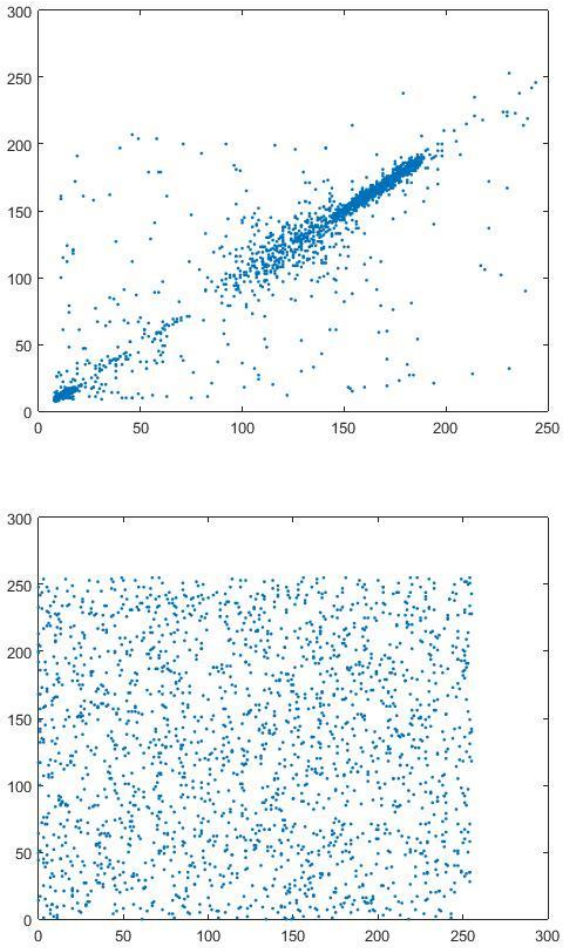


Fig. 7: Correlation between the adjacent pixels horizontally of the plaintext image and the encrypted image.

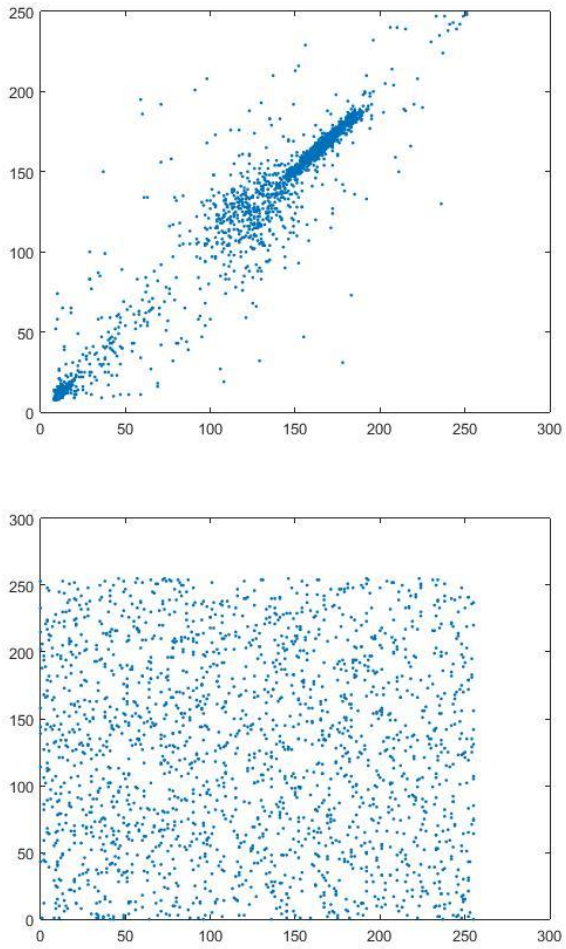
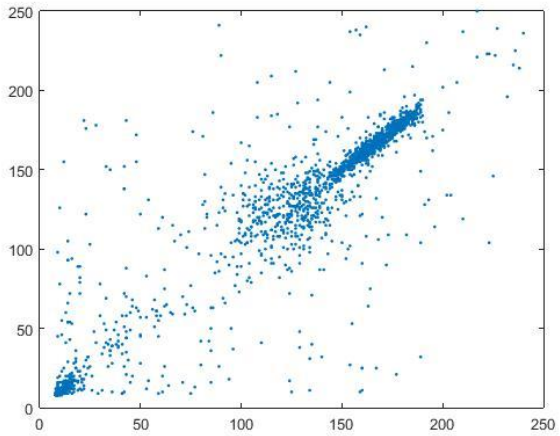


Fig. 8: Correlation between the adjacent pixels vertically of the plaintext image and the encrypted image.



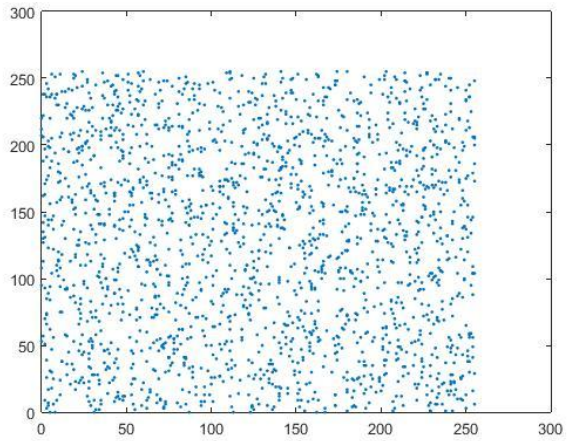


Fig. 09: Correlation between the adjacent pixels diagonally of the plaintext image and the encrypted image.

Fig.7, Fig.8 and Fig.9 show the correlation between the adjacent pixels of the plaintext and encrypted image. After calculating the correlation coefficient (Tab 03), we see that the neighboring pixels in the plaintext image have a strong correlation (coeff $\approx$ 1), whereas in the encrypted image there is a very weak correlation (coeff $\approx$ 0). This weak correlation between neighboring pixels in the encrypted image makes our cryptosystem resistant to statistical attack.

Image Cameraman.tif	**Direction**		
	Horizontal	**Vertical**	**Diagonal**
Plaintext Image	0.9505	0.9628	0.9098
Encrypted Image	- 0.0132	0.0027	-0.0083

Tab. 3: Correlation coefficient

c.4 Key size :

Main-key : 122 678 785 nucleotide bases.

Sub-key :

- Pos_Start = [1 … 122 678 785] $(122 * 10^6) \approx 2^{27}$.
- Nbr_Base = [1 … 122 678 785] $(122 * 10^6) \approx 2^{27}$.
- Iindex I = [1 … 122 678 785] $(122 * 10^6) \approx 2^{27}$.
- Numbre of round NR = [1..56] (2^6)

Key size = 27+27+27+6 = 87 bits

III. RELATED WORK

As DNA encryption has been cited as one of the safest methods of data representation, new algorithms have been developed by researchers to ensure data security. This section presents some algorithms that use DNA for encryption.

Hereby, we give examples of the several well-know that can be found in literature.

One of the algorithms suggested using a bi-serial DNA encryption method in which the plaintext is converted

to hexadecimal code and into a binary code. This message is divided into two parts; one will be used as a key and the other as a message. The XOR operation is also performed in order to increase the compression factor. A DNA encoded message is received after the application of the digital DNA coding, then the PCR amplification is implemented using two main pairs as the key and the compression is performed for a variable data length [3].

Al-Wattar et al have proposed other DNA based methods dependent on the key for the MixColumns and ShiftRows transformations involved in the AES algorithm, which has similar characteristics to those of the original AES algorithm. Increasing its resistance against attacks. [4][5].

Another algorithm proposed by Shreyas Chavan was plaintext encryption using a DNA-based method and a One Time Pad (OTP). This algorithm uses two keys. One of the keys is a random string of nucleotides forming a DNA sequence, its length depends on the length of the plaintext. The second key is the binary sequence used for OTP, its length is twice that of the DNA sequence key [6].

Varma and Raju have analyzed the different approaches of DNA encryption based on the matrix manipulation and the secure key generation scheme. [7].

Kang Ning suggested an idea of securing data by a method called pseudo-cryptography DNA method. The principle suggested in this method is to convert text into protein according to the table of genetic codes. [8].

Kritika Gupta and Shailendra Singh proposed algorithm that included the conversion of plaintext into its ASCII code, which was then converted to a binary form. Then, these binary values are encoded in DNA sequences. After that, a DNA sequence is selected as a key and grouped into 8-character blocks. Depending on the positions of the characters in the key, a table is created and, using this table and key, the produced data is converted into an encrypted form [9].

IV. Conclusion:

The algorithm proposed in this paper is a symmetric algorithm with block cipher encryption. It is based on 03 essential points:

1- A non-unique coding of the nucleotide bases which varies according to the number of occurrences of each base.

2- A logical XOR operation between the obtained coded key and the plaintext in its binary form.

3- A confusion of the result by using a permutation box with a certain number of rounds obtained by a sub-key.

The robustness of this cryptosystem is based on the coding of nucleotide bases is variable.

Finally, future research is needed to further improve the efficiency and performance of DNA encryption to ensure better security of the encrypted result.

REFERENCES

[1] Leonard Adleman, "Molecular Computation of Solutions to Combinatorial Problems," *Science*, 266:1021-1024, November 1994.

[2] T. Mandge and V. Choudhary. A review on emerging cryptography technique: DNA cryptography. International Journal of Computer Applications (IJCA), Vol. 13, pp. 9-13, February 2013.

[3] D.Prabhu, M.Adimoolam, "*Bi-serial DNA Encryption Algorithm*"[Online]. https://pdfs.semanticscholar.org/1754/f0eb5852500598a70af4002e186cd2f3c6ce.pdf

[4] A. H. Al-Wattar, R. Mahmod, Z. A. Zukarnain, and N. Udzir. A new DNA based approach of generating key dependent MixColumns transformation. International Journal of Computer Networks & Communications (IJCNC), Vol. 7, No. 2, pp. 93-102, March 2015.

[5] A. Al-Wattar, R. Mahmod, Z. Zukarnain, and N. Udzir, "A new DNA based approach of generating keydependent ShiftRows transformation. International Journal of Network Security and Its Applications (IJNSA), Vol.7, No.1, January 2015.

[6] Shreyas Chavan, "*DNA Cryptography Based on DNA Hybridization and One Time pad scheme*", International Journal of Engineering Research & Technology, Volume 2 Issue 10, October-2013.

[7] P. S. Varma, K. G. Raju. Cryptography based on DNA using random key generation scheme. International Journal of Science Engineering and Advance Technology (IJSEAT), Vol. 2, Issue 7, pp. 168-175, July, 2014.

[8] Kang Ning, "*A Pseudo DNA Cryptography Method*", arXiv:0903.2693 [cs.CR], Cornell University Library, March-2009.

[9] Kritika Gupta, Shailendra Singh, "*DNA Based Cryptographic Techniques: A Review*", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3 Issue 3, March 2013.

Image encryption by AES algorithm based on chaos-Permutation

Rachid RIMANI
University Mustapha Stambouli of MASCARA
LACOSI Laboratory
ALGERIA
rachid.rimani@univ-usto.dz

Naima HADJ SAID
University of Sciences and Technology of Oran Mohamed Boudiaf
USTOMB – ALGERIA
naima.hadjsaid@univ-usto.dz

Adda ALI-PACHA
University of Sciences and Technology of Oran Mohamed Boudiaf
USTOMB – ALGERIA
a.alipacha@gmail.com

Juan Antonio López RAMOS
Department of Mathematics
University of Almeria

SPAIN
jlopez@ual.es

***Abstract*: Today, in particular with the development of the internet, transmitting confidential information in a secure manner has become a basic need; data encryption is often the only effective way to meet these requirements. Traditional cryptography is the study of methods for transmitting confidential data; in modern cryptography, transformation is applied to the plain message that makes it incomprehensible; these transformations are mathematical functions, called cryptographic algorithms, which depend on a parameter called key.**

In this paper, we presents a new symmetrical crypto-system by block for encrypting images on using the encryption AES algorithm (Advanced Encryption Standard) combined with the CBC mode (Cipher Block Chaining) in order to improve the security level. The proposed crypto-system consists on replacing the linear permutation of ShiftRows step of the AES encryption algorithm by a nonlinear and random permutation, this permutation is calculated by a chaotic sequel.

Keywords: AES algorithm, chaotic sequel, encrypting images, non-linear permutation, random permutation, symmetrical crypto-system.

I. INTRODUCTION

Cryptography is a mathematical technique that allows the transmission of confidential data on an unsecured medium without an intruder discovering the content. These data will be decrypted only by the recipient or the one knowing the encryption key. Cryptography guarantees, among other things, integrity, non-repudiation and the authenticity of the data in addition to confidentiality [1]; currently, several cryptographic systems have emerged to solve new security issues such as access to information, communications between computers, e-commerce, etc.

Encryption algorithms can be separated according to the encryption technique in two main categories: per block or per stream. Block cipher is the most appropriate for encrypting images because of their size and their information which is two-dimensional in nature and at times redundant. Therefore, we use the block cipher in our crypto-system.

The iterative encryption algorithms by block are essentially divided into two major structures. According to the architecture of the internal iteration function, the two mainly used structures are: the Feistel scheme (used in DES and RC6), and substitution-permutation network structure SPN (used in AES). In addition, each structure can be fixed (fixed key for each iteration) or variable (dynamic key with iterations). It is clear that the variable structure that depends on the iteration keys is more difficult to study by the attacker, and for this reason, we adopt it for the proposed crypto-system.

In order to build a secure encryption system, Shannon [2] set out two fundamental principles to respect, which are confusion and diffusion. Confusion is provided by a non-linear substitution, and the diffusion technique is often realized by the permutations of blocks, pixels or binary permutations [3], [4]. Examples of algorithms that apply permutations are various, we quote DES, AES, RC4 [5], etc. We introduced in this paper a new permutation technique to ensure the diffusion, whose principle is to replace the linear permutation of ShiftRows step of the AES encryption algorithm by a nonlinear and random permutation, which varies according to the chaotic sequel already generated. The use of the CBC mode allows to guarantee that even if the gross image contains many identical blocks, each of them will be encrypted differently.

II. STRUCTURE OF AES [6] [7]

The AES (Advanced Encryption Standard) is a symmetric encryption algorithm that processes data blocks of 128, 196 or 256 bits and the size of the typically key used is 128 bits with variants of 192 and 256 bits. The data blocks and the key are stored in a table as shown in Figure 1; the number of columns depends on the blocks size and the key.

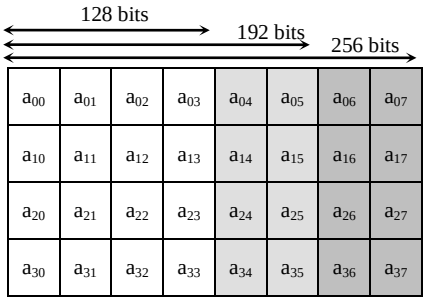


Figure 1. State table block

AES is based on a succession of rounds; the number of rounds varies depending on the block size and the key size according to the table 1.

TABLE I. The number of rounds according to | K | and | B |

	|K| =128	**|K| =192**	**|K| =256**
|B| =128	10	12	14
|B| =192	12	12	14
|B| =256	14	14	14

|K| : Key size ; |B| : block size

In our case, we will use the AES algorithm for a 128 bits block size with a 128 bits key size also giving a number of rounds r equal to 10.

The AES algorithm in the encryption mode consists of 3 steps:

• The first is an " exclusive or" operation between the plaintext block and the secret key K.

• The second step is a set of 9 rounds each executing 4 operations: SubBytes, ShiftRows, MixColumns and AddRoundKey.

• The last step is a round in which the MixColumns operation is not performed.

All the encryption operations are invertible. Therefore, in order to decrypt a block, we apply operations reversely.

III. CONTRIBUTION: IMAGE ENCRYPTION BY AES ALGORITHM WITH CHAOS-PERMUTATION

Images encryption is provided by the AES algorithm replacing the permutation of ShiftRows step by the permutation table obtained using a logistic map method (logistic chaos of parameter μ, X0 and F) to generate a sequence st of pseudo-random numbers without repetition modulo (depending on key size). fig 2, fig 3

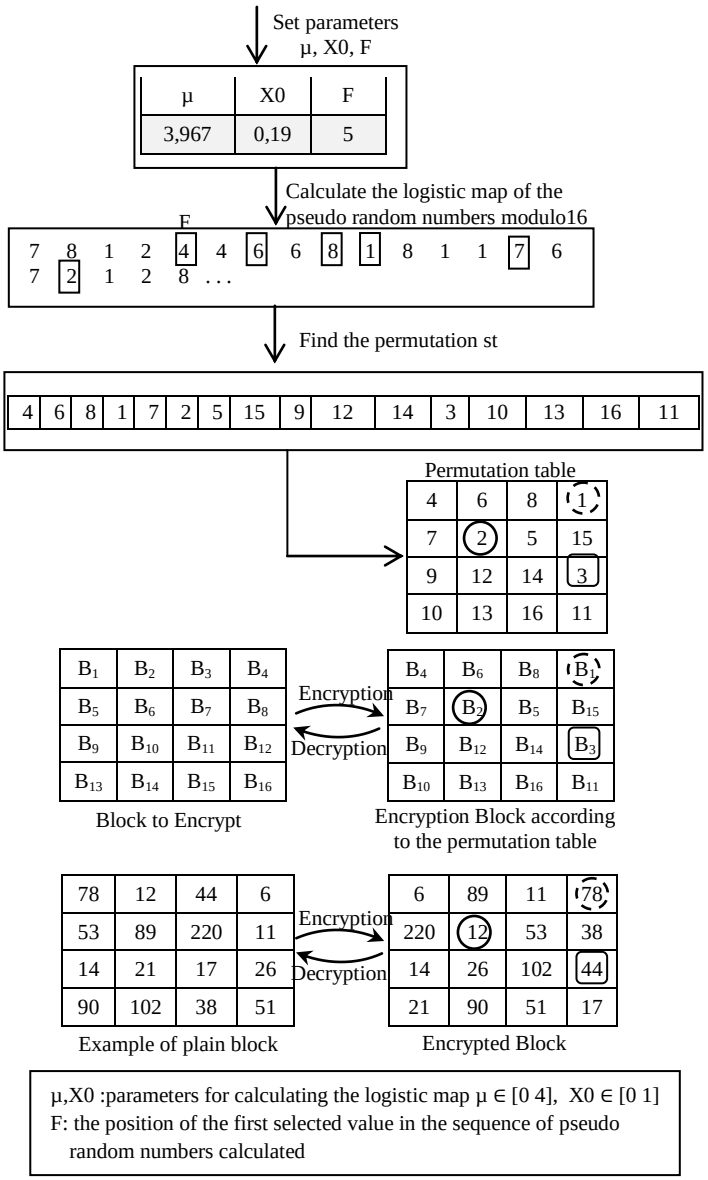


Figure 2. Encryption/decryption using of the permutation table

the recipient must calculate the permutation *st* using the same shared parameters *μ, X0* and *F* to have the permutation table; so to decrypt a block, the same procedure is applied reversely. When the image contains homogeneous areas, all identical blocks will also be identical after encryption. In this case, the ciphered image contains textured areas and the entropy of the image is not maximal. To solve this problem, we applied the CBC mode on our algorithm; this allows on one hand to increase the level of complexity and on the other hand satisfies second Shannon's theory of diffusion.

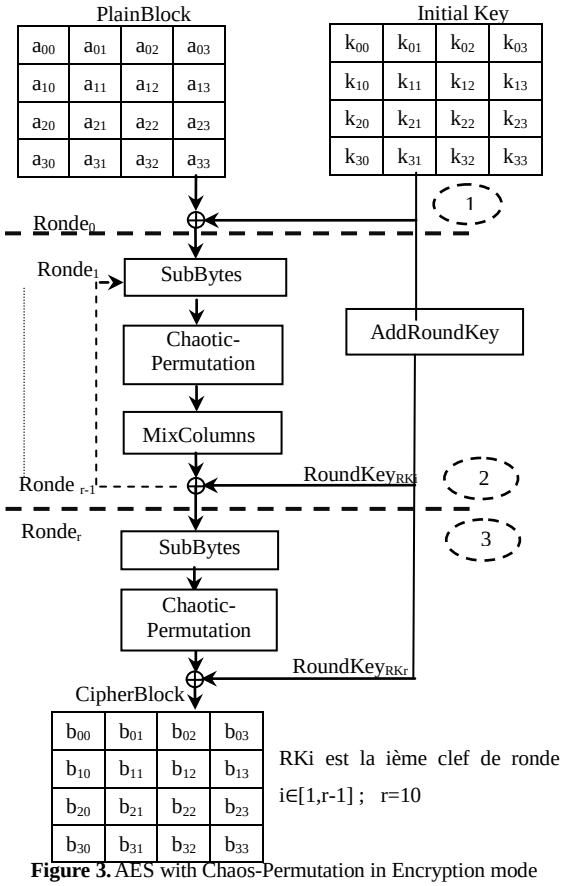


Figure 3. AES with Chaos-Permutation in Encryption mode

IV. Security Analysis of Proposed Crypto-System and Experimental Results

After the encryption of an image, we must have an independence (low correlation) between the original image pixels and that of the ciphered image. This independence can be seen by simple viewing of the ciphered image, but the visual inspection remains insufficient to judge the encryption of an image. The metrics for evaluating the degree of encryption can be classified into statistical analysis, differential analysis and sensitivity analysis of the secret key.

IV.1. Statistical analysis

To resist the statistical attack, the histogram of the ciphered image must be very close to a uniform distribution (Figure 4.e). To measure this uniformity, we apply two tests, the first test is chi-square and the second test is entropy.

A. Chi-square test

The chi-square test is given by the following relation:

$$X^2_{exp} = \sum_{i=0}^{Q-1} \frac{(O_i - e_i)^2}{e_i} \qquad (1)$$

The distribution of the histogram is uniform if it satisfies the following condition:

$X^2_{exp} < X^2_{th\ Q-1,\ \alpha} = 273{,}12$ for a threshold α fixed at 0.05 in our experiment.

In our case we found X^2_{exp}=259.7449

B. Entropy test

The entropy test of an image *M* is given by equation 2:

$$H(M) = \sum_{i=0}^{Q-1} p_i log_2 \frac{1}{p_i} = -\sum_{i=0}^{Q-1} p_i log_2 p_i \qquad (2)$$

In the case of a uniform distribution, the entropy *H(M)* is maximum and is given by equation 3 :

$$H_{max} = log_2(Q) = 8 \qquad (3)$$

Thus, if the value of entropy is very close to H_{max}, it means that the source data has a nearly uniform distribution and the crypto-system providing such data can withstand the statistical attack.

Figure 4 shows the results of Lena's image 224x224, encrypted by the AES algorithm with Chaos-Permutation in CBC mode.

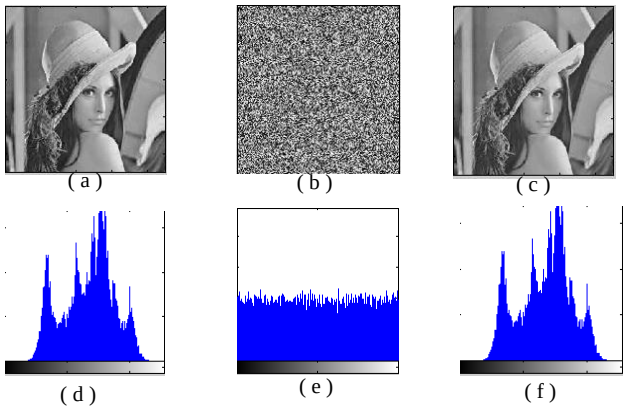


Figure 4. Encryption and decryption image by AES algorithm with Chaos-Permutation in CBC mode

a) Plain image
b) Ciphered image
c) Decrypted image
d) Histogram of image (a)
e) Histogram of image (b)
f) Histogram of image (c)

We notice that the ciphered image is not visible anymore. Comparing the plain image histogram with the ciphered image histogram, we note that the occurrence probabilities of each gray level are uniformly distributed with a very high entropy of ciphered image (close to 7.9963).

Table 1 indicates that the entropy of the AES algorithm with Chaos-Permutation is large compared to the AES algorithm; we also note that the entropy of the AES algorithm with Chaos-Permutation in CBC mode is high compared to the algorithm without CBC mode, so we can say that we have added complexity by CBC mode.

TABLE 1. Comparison of entropy between AES encryption algorithm and Chaos-permutation with and in CBC mode

Algorithm	Entropy Plain	Entropy Cipher
AES in CBC mode	7.2353	7.9961
Chaos-Permutation in CBC mode	==	7.9963

C. Correlation coefficient of adjacent pixels

The calculation of the correlation coefficient between the pixels allows evaluating the encryption quality of crypto-system. Generally, in an original image, each pixel is strongly correlated with its adjacent pixels in the three directions horizontal, vertical and diagonal. An ideal cryptosystem should produce encrypted images without any correlation between adjacent pixels.

To test the correlation between adjacent pixels; we took 5300 pairs of two adjacent pixels from the original image and those encrypted in the three directions horizontal, vertical and diagonal as follows:

For each selected pixel (at the number 5300) of coordinates *(i, j)* we form 4 vectors V, V_H, V_V, V_D containing the gray levels of the pixels which are found at the positions *(i, j), (i+1, j), (i, j+1), (i+1, j+1)* respectively. The correlation coefficients in the three directions are C_{VH}, C_{VV}, C_{VD}.

Table 2 groups the correlation coefficients for the following algorithms: the proposed algorithm AES with Chaos-Permutation, ECKBA proposed in [8] (it was cited and described as references for several proposals of image encryption algorithm [9], [10], [11], [12]) and the algorithm proposed by Mansour et al [13]. We notice that the correlation coefficients measured for the original image are close to 1, while the correlation coefficients for the encrypted images of different algorithms are close to 0, it is also deduced that the encryption has considerably attenuated the correlation between pixels of encrypted images.

TABLE 2. Correlation coefficient of adjacent pixels

	Correlation coefficient		
Direction	**HORIZON-TAL**	**VERTI-CAL**	**DIAGO-NAL**
Plain image	0.9244	0.9588	0.8948
Chaos-Permutation	-0.0021	0.0143	0.0085
ECKBA	0,0760	0,0227	-0,0012
Mansour et al	0,0479	-0,0414	-0,0416

In order to compare the performances of the proposed algorithm with ECKBA and Mansour et al algorithm, we have plotted the graph in Figure 5, which represents in absolute value the correlation coefficients of the adjacent pixels of the encrypted images of each algorithm.

We note that for the horizontal and vertical direction, Chaos-Permutation performance has exceeded the other two algorithms; with the exception of the ECKBA algorithm which has a value of diagonal adjacent pixels lower than the proposed algorithm.

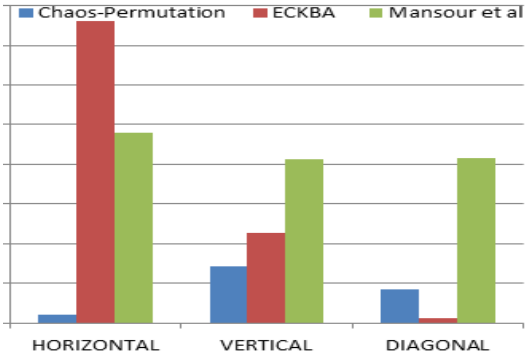
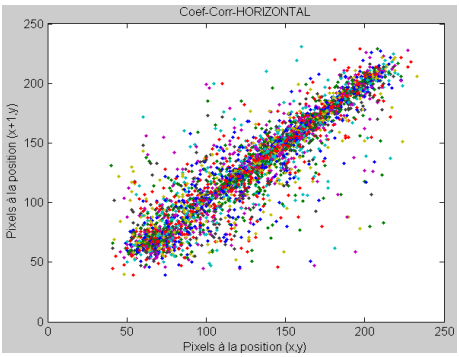
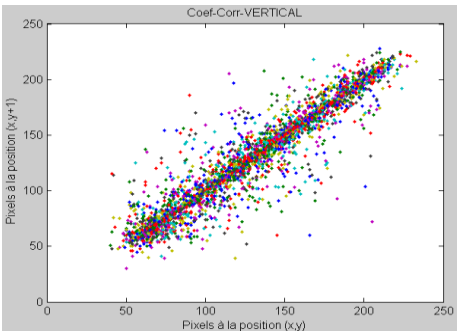


Figure 5. Correlation coefficient comparison of adjacent pixels for different algorithms

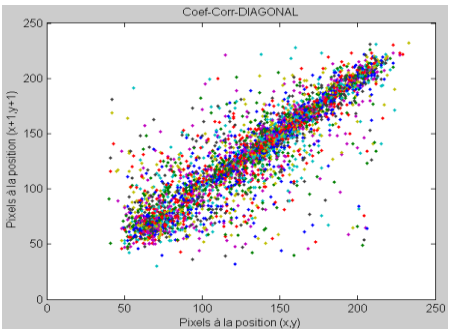
Figure 6 represents the correlation distributions of the horizontal, vertical and diagonal adjacent pixels in the original image. We note that the pixel intensity distribution is focused on the diagonal; the pixels are then strongly correlated.



(a)



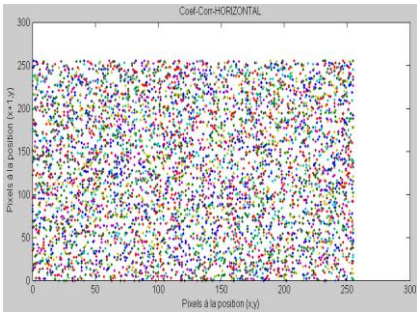
(b)



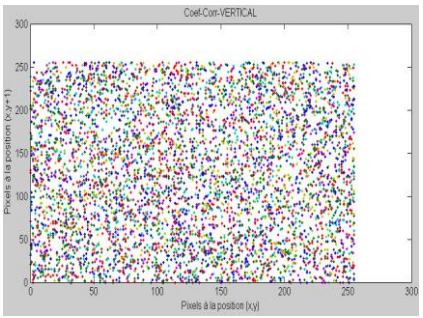
(c)

Figure 6. Correlation distribution of peers of adjacent pixels in the original image:
a) Horizontally, b) Vertically, c) Diagonally)

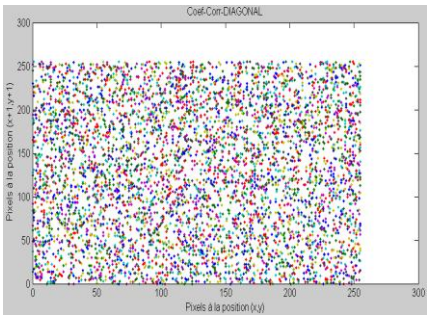
Figure 7 represents the correlation distributions of the horizontal, vertical and diagonal adjacent pixels in the encrypted image. We note that the pixel intensity distributions are uncorrelated and they have a uniform distribution.



(a)



(b)



(c)

Figure 7. Correlation distribution of peers of adjacent pixels in the encrypted image:
a) Horizontally, b) Vertically, c) Diagonally

All results show that the crypto-system used reveals good properties and resists against statistical attacks.

IV.2. Differential analysis

To ensure the security of an image encryption scheme against differential analysis, two quantitative measures are used: the Number of Pixels Change Rate (NPCR) and the Unified Average Changing Intensity (UACI) defined by the following equation:

$$NPCR = \frac{\sum_{i=0}^{M-1}\sum_{j=0}^{N-1} D(i,j)}{M * N} * 100 \quad (4)$$

$$UACI = \frac{1}{M * N}\sum_{i=0}^{M-1}\sum_{j=0}^{N-1}\frac{|I_1(i,j) - I_2(i,j)|}{255} * 100 \quad (5)$$

Table 3 indicates that the NPCR / UACI score between original image and encrypted image by the Chaos-Permutation algorithm is large compared to that of AES.

We also note that the NPCR of the proposed algorithm is large compared to the ECKBA encryption algorithm and the algorithm proposed by Mansour et al. The UACI of the proposed algorithm is better than the other tested algorithms.

TABLE 3. NPCR and UACI values between the original image and the encrypted image

Algorithm	NPCR (%)	UACI (%)
AES	99.5556	15.2373
Chaos-Permutation	99.6293	15.4133
ECKBA	99.5625	13.4146
Mansour et al	99.5937	13.0731

We performed another test between two encrypted images (LENA 224*224) that differ from the original image by a single pixel, the NPCR and UACI values are shown in table4.

TABLE 4. NPCR and UACI values between two encrypted images having one pixel different at the origin

Algorithm	NPCR (%)	UACI (%)
AES	0.0319	0.0091
Chaos-Permutation	0,0319	0,0104
Chaos-Permutation in CBC mode	56,1683	18,8875
ECKBA	100	15.9849
Mansour et al	0.0156	0.0059

Note that we have obtained the same NPCR compared to the AES algorithm, but the UACI value by the algorithm the Chaos-Permutation in CBC mode is the best. We also note that the NPCR of the ECKBA algorithm reaches the maximum value but its UACI value remains lower than the proposed algorithm.

V. SENSITIVITY OF THE SECRET KEY

To test the sensitivity of the key on our crypto-system and therefore the reliability of the proposed approach; we did two different tests:

- The first test is to encrypt the same image by two keys slightly different; the used keys are different only by a single bit at the initial condition.

K1=[9 17 43 74;36 20 85 13; 41 7 16 54;21 47 63 **95**] 0**1**011111

K2=[9 17 43 74;36 20 85 13; 41 7 16 54;21 47 63 **31**] 0**0**011111

The figure 8 contains the histograms of Lena's image (224x224) encrypted by the two keys K1 and K2.

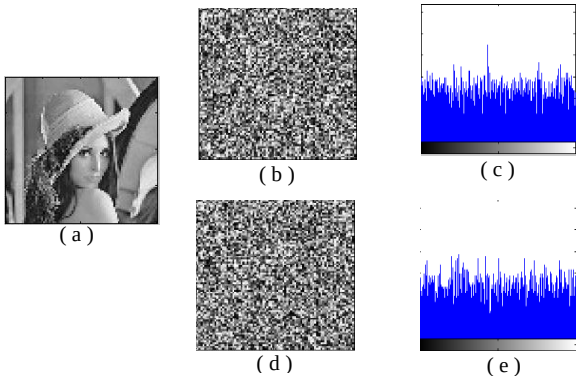


Figure 8. Image encrypt by two slightly different keys K1 and K2
a) Plain image
b) Ciphered image with K1, d) Ciphered image with K2
c) Histogram of image (b), e) Histogram of image (d)

Changing a single bit in the encryption key then gives two completely different histograms with a very low correlation coefficient between the two encrypted images (corrcoef = 0.0080). Therefore, the two encrypted images are completely independent from each other.

- The second test consists on using the key K1 to encrypt an image (LENA 80x80), and using the key K2 in the decryption phase. (Figure 9)

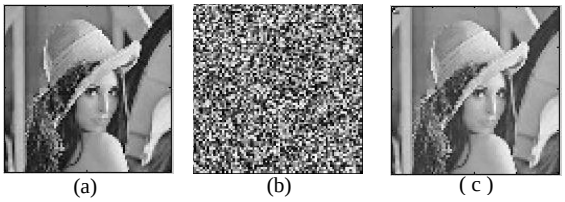


Figure 9. a) Plain image, b) Image decrypted by K2
c) Image decrypted by K1

We notice that the decryption process failed when the secret key is slightly changed and the decrypted image is completely blurred (Figure 9. b).

With these two tests, we conclude that the AES algorithm with Chaos-Permutation is extremely sensitive to small changes of the secret key, so we can say that the proposed approach guarantees security against brute force attacks.

VI. AVALANCHE CRITERION

Any function that satisfies this criterion must have a change with a probability of one-half of the output bits, if only one bit at the input changes. The output will then be uniform and no statistical prediction can take place [14], [15], [16], [17].

VI.1. Calculation of the Hamming distance

The Hamming distance is the number of different bits between two binary sequences C1 and C2, which will be noted d_H(C1, C2). This criterion measures the avalanche effect and it is defined by the equation 6:

$$d_H(C_1, C_2) = \sum_{i=0}^{n-1} |C_1(i), C_2(i)| \qquad (6)$$

We encrypted two binary sequences E1 and E2, which differ by a single bit by our algorithm AES with Chaos-Permutation, then we calculated the Hamming distance between the two resulting encrypted sequences C1 and C2, by changing each time the position of the bit to be changed for plain text sequences. Figure 10 shows the percentage of the Hamming distance in bits given by equation 7:

$$pd_H(j) = \frac{d_H(j)}{L_b} * 100 \qquad (7)$$

The size of the binary sequences tested is L_b = 128 bits and j represents the different bit position. We obtain 78.91% pairs of encrypted sequences with a Hamming distance greater than 46%, and 21.09% pairs having a distance less than 46%; the average value of the Hamming distance obtained for our algorithm is 49.6338 (Figure 10); indeed whatever the position of the changed bit, this provided almost 50% of difference between the bits of two concerned sequences. So we can say that the avalanche property is reached by the algorithm AES with Chaos-Permutation.

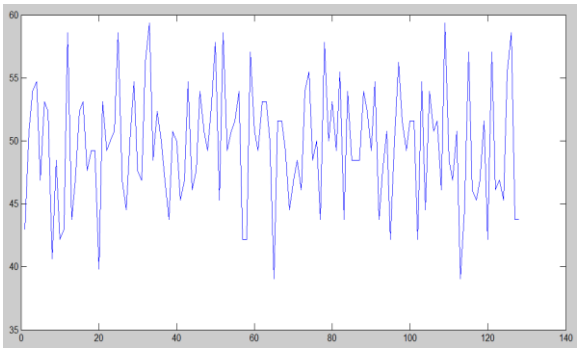


Figure 10. Percentage in bits of the Hamming distance according to the positions of the changed bits for pairs of encrypted texts by AES Chaos-Permutation

VII. CONCLUSION

We have introduced in this work a new crypto-system in order to replace the linear permutation of the ShiftRows step with a random and nonlinear permutation. Another drawback in ShiftRows step is the public permutation; on the other hand, in the proposed approach, the permutation procedure is secret; this means that the security in the Chaos-Permutation method is not based on the encryption scheme, but on the confidentiality of shared parameters F, μ and X0 of the logistic map.

For the chaos, the logistic map was used as an example for generating a pseudo random numbers, but if necessary, we look for another card, which will have best properties such as PWLCM.

The proposed algorithm is suitable for images, audio, text; and if we change the size of the bloc, the encryption/ decryption procedure does not change; it is sufficient to modify the size of the permutation table.

In conclusion, we can say that the modification made on the AES algorithm does not have any influence in its efficiency, but also enhances its fortress as can be observed in the entropy and other values obtained.

REFERENCES

[1] A. Menezes, P. VanOorschot, S. Vanstone, Handbook of applied cryptography, 1997 by CRC Press.

[2] Claude E. Shannon, Communication Theory of Secrecy Systems. Bell System Technical Journal, 28(4) : p. 656-715, November 1949.

[3] Yanbing Liu, Simei Tian, Wenping Hu, Congcong Xing, "Design and statistical analysis of a new chaotic block cipher for Wireless Sensor Networks", Communications in Nonlinear Science and Numerical SimulationVolume 17, Issue 8, Pages 3267–3278, August 2012.

[4] Bruce Schneier, Applied cryptography : protocols, algorithms, and source code in C (cloth), john wiley & sons,inc, janvier 1996,

[5] RSA Security. http ://www.rsasecurity.com/. 2003.

[6] J. daemen, and V. rijmen, "AES proposal: the rijndael block cipher," technical report, proton world int. l, katholieke universiteit leuven, esatcosic, belgium, 2002.

[7] William stallings, "cryptography and network security principles and practice," pearson, united states of america, p. 900, 2011.

[8] D. Socek, S. Li, S. S. Magliveras, B. Furht, "Enhanced 1-D Chaotic Key Based Algorithm for Image Encryption," IEEE, Security and Privacy for Emerging Areas in Communications Networks, 2005.

[9] Abir Awad, Safwan El Assad, Daniel Carragata , "A Robust Cryptosystem Based Chaos for Secure Data", IEEE, ISIVC Conference On, Image/Video Communications over fixed and mobile networks, Bilbao Spain, July 2008.

[10] Marwa Abd El-Wahed, Saleh Mesbah, and Amin Shoukry , Efficiency and Security of Some Image Encryption Algorithms, Proceedings of the World Congress on Engineering Vol I WCE, July 2 - 4, London, U.K, 2008.

[11] Hassan Noura, Safwan El Assad Calin Vladeanu, Daniel Caragata, An Efficient and Secure SPN Cryptosystem Based on Chaotic Control Parameters 6th International Conference on Internet Technology and Secured Transactions, Abu Dhabi, UnitedArab Emirates, 11-14 December 2011.

[12] Mintu Philip, Asha Das, Survey: Image Encryption using Chaotic Cryptography Schemes, IJCA Special Issue on Computational Science - New Dimensions & Perspectives NCCSE, 2011.

[13] Ismail Mansour, Gerard Chalhoub, Bassem Bakhache, "Evaluation of a fast symmetric cryptographic algorithm based on the chaos theory for wireless sensor networks", MWNS (International Symposium on Mobile Wireless Network Security, Liverpool, UK, 25-27 June, 2012.

[14] Adams C, Tavares S. Good S-boxes are easy to find. In: Advances in cryptology: Proceedings of CRYPTO'89. Lecture Notes in Computer Science, p. 612–5, 1989.

[15] Rohiem, A.E.; Elagooz, S.; Dahshan, H , "A novel approach for designing the s-box of advanced encryption standard algorithm (AES) using chaotic map",Radio Science Conference, 2005. NRSC 2005. Proceedings of the Twenty-Second National Volume, Issue, 15-17, Page(s):455– 464, March 2005.

[16] On the design of S-Boxes A.F Webster and S. E Tavares, Copyright © 1998, Springer- Verlag, 1998.

[17] A. Benjeddou, A.K. Taha, D. Fournier-Prunaret, R. Bouallegue, "A New Cryptographic Hash Function Based on Chaotic S-box", CSNDSP, Austria, 23-25 July, 2008.

New Technique of styganography Based on the Theory of Chaos : Survey

A. Bouguessa
Coding Laboratory
and Information Security,
USTO University,
Oran, Algeria
abdelkader.bouguessa@univ-usto.dz

N. Hadj said
Coding Laboratory
and Information Security,
USTO University,
Oran, Algeria
naima.hadjsaid@univ-usto.dz

A. Ali Pacha
Coding Laboratory
and Information Security,
USTO University,
Oran, Algeria
a.alipacha@gmail.com

***Abstract*—Today with increasing use of the Internet and network devices, there is an increase in the demand for more secure data communication. This problem has led to the development of hybrid security mechanisms. Various techniques are available in the literature which makes use of different encryption and steganography mechanisms which has certain advantages and disadvantages. In this work, we give a state of the art on the three notions in order to propose a new hybrid security system that tries to choose the best mechanism of cryptography and steganography. In addition, to increase the capacity of the proposed system it is proposed to use a compression technique..**

***Index Terms*—Hybrid system; Compression; cryptography; steganography; Huffman; chaos; LSB.**

I. Introduction

Currently, with the evolution of the internet and network devices such as increased use of smart phones and communication tools, this leads to a strong demand for robust and more secure data communication, this problem has leads the researchers to develop new security mechanisms from the combination of cryptography and steganography, or both covers the disadvantages of each other and improve the overall security of communication. In a hybrid mechanism, cryptography and steganography are involved throughout the process (see Figure 1).

The data is first encrypted using an encryption technique, then it is embedded in a cover object using a steganography technique. Figure 1 shows the basic architecture of the hybrid security mechanism. The basic features are as follows: The message is first encrypted with the secret key, and this encrypted message is then embedded in the coverage object using the Steganography technique, resulting in the creation of a stego object that contains the secret data.

To extract the data the inverse process is also represented in the figure. First, the encrypted data is extracted from the stego object using the reverse steganography and then these encrypted data are decrypted using the secret key and a system of decryption to get the original data. On the other hand, our work presented in this paper proposes a new hybrid system that tries to combine the best cryptographic technique with the best steganography technique.

The rest of the document is organized as follows. Section II gives the background of this document. Section III describes our motivation and the main challenges we face. Section IV provides an overall picture of our proposal that represents a general approach to significantly strengthen the steganography process based on chaos. Finally, Section V concludes this document and establishes our future work plan.

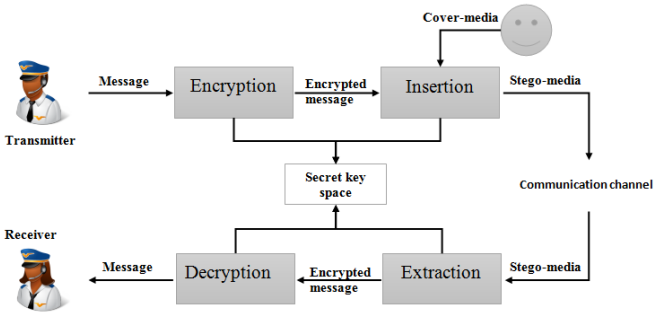


Figure 1. Basic principle of hybrid security mechanism.

II. Context

The next section gives a detailed overview of the three basic terms of our work, compression, cryptography and styganography.

A. Data compression

Compression is the process of reducing the amount of data used to represent a file without overly reducing the quality of the original data. It also reduces the number of bits required to store and transmit digital media [1]. There are some techniques in goal acquisition, one of them is to reduce the redundant information in the file. Another is simply throwing away the least important parts of the data and keeping the most important ones.

1) Representation of digital data: The digital data consists of a sequence of symbols from a set of finite alphabets. For data compression to always contain meaningful information, there is a standard representation of the original data that encodes each symbol using the same number of bits. For a text file, for example, each symbol is represented by an ASCII

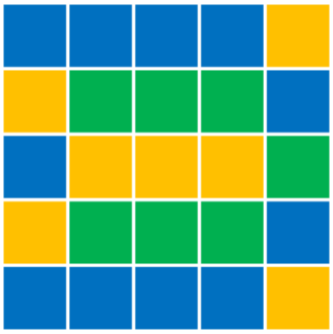


Figure 2. Simple colorful 5 x 5 grid image.

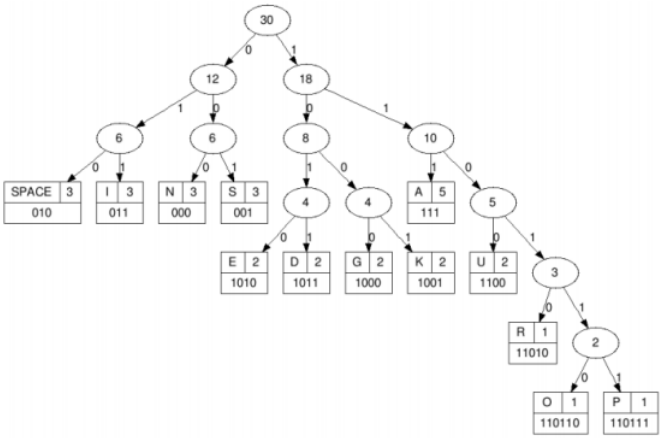


Figure 3. Huffman tree for the string and the corresponding code for each symbol.

code, which is a one byte long code that corresponds to each symbol of a standard keyboard.

Data compression is successful when the compressed data can be represented by shorter codes on average than the original data. So for compression to be meaningful, there must be a standardized representation for data compression.

2) Types of data compression: There are two main classifications of data compression based on information retention.

- Lossy compression means that some information is lost during the compression process. Lossy compression is based on the fact that there are certain limitations on what human sensory capacity can and can not perceive. Thus, some small information in the file whose human presence can not really say can be deleted. It is commonly used in compression of multimedia files such as MPEG and MP3 compression.
- Lossless compression means that no information is lost during the compression process. When the data is uncompressed, the result is perfectly matched bit by bit with the original data. Compressed data uses less space than the original data, but no information is removed, making it more efficient. An example of a program that uses lossless compression is the popular Win ZIP compression program . An example of lossless data compression is Huffman coding.

3) Techniques of Data compression :

- Simple repetition simply replaces a series of successive symbols that take place in a sequence with another token or flag. For example, 3196070000000000000000000000000000 can be replaced by 319607z30. The symbol 'z' is the flag for zero. The simple repeat application includes zero length deletion (as the example above), silence in audio files, bitmap images, and spaces (spaces, newline symbols, or tabs) in the text files.
- The Run-Length or RLE encoding is the method to rewrite the data as pairs of values (v, n) with v is the value (for example, in the case of an image, the color value) and n is the number of successive occurrences. For example, see Figure 2. First, a symbol is assigned to each of the colors, B for blue, Y for yellow and G for green. The image is stored with the symbol representation, that is, BBBBYYGGGBBYYYGYGGGBBB B Y. The image size is 25 characters.
  Now, RLE is applied to the representation of the symbol using the pairs of values (vi, ni). For example, the first recurring color is 4 blocks of blue. For these 4 blocks of blue, the pair is (B, 4). For all data, the result is (B, 4), (Y, 2), (G, 3), (B, 2), (Y, 3), (G, 1), (Y, 1), (G, 3), (B, 5), (G, 1). To store this compressed data, the representation is B4Y2G3B2Y3G1Y1G3B5G1, which is 80% of the original size. The disadvantage of RLE is that if the image or data is too irregular or too noisy, the compression may produce larger data than the original. RLE is used as a complementary method in JPEG compression.
- Huffman coding, first introduced by David A. Huffman in 1952, is a lossless compression algorithm. The concept is to assign some variable length codes to enter characters. The length of the code is based on the frequency of its corresponding characters. Character with the presence of most gets shorter code and the one with the occurrence minus the longer code. In order to achieve an efficient and unambiguous set of code for a specific set of input characters, there are certain restrictions in the coding. The following basic restrictions will be imposed on an overall code :
  - There will not be 2 messages consisting of identical coding provisions.
  - The message codes will be constructed such that there is no need for further indication to specify where a message code begins and ends once the starting point of a message sequence is known.

  As Huffman [1] stated, the restriction (b) does not require this message to be encoded in such a way that its code appears, the digit for the digit, as the first part of any longer message code. . It must declare that no code should be a prefix code of any other code.

1) Prefix codes : To understand the prefix codes, look at this small example below. That there are four input

characters A, B, C, D, one of their corresponding code 0, 1, 00 and 01 respectively. This coding mode leads to ambiguity since the character code A is a prefix of the codes assigned to C and D. For example, if the result of the compression is 00100100, the original decompressed data could be CBADC, AABCAD, ADADC or some other possibilities. Now let's see another way to assign the code. Assign the codes 00, 01, 10, 11 to the characters A, B, C and D. If we get the same compression string as above (00100100), we can be sure that the uncompressed original data is ACBA. There is no ambiguity in this coding.

2) Generation of a Huffman tree : An effective way to assign codes to a set of input characters is to use a Huffman tree. A Huffman tree is a binary tree to determine which code should be assigned to which character. The algorithm for generating a Huffman tree for a text file, referring to 3, is as follows.
   - Count the frequency of occurrence of each symbol in the text.
   - Take two symbols with the least number of occurrences (for example, P and Q which, for example, have a probability of 1/7 each) and treat both as parent nodes.
   - Make parent nodes from these two nodes so that there is a new PQ symbol with a probability of 1/7 + 1/7 = 2/7.
   - Take the following two symbols, including the new symbol, with the fewest occurrences. Do step 3 so that another new symbol with its probability is acquired.
   - Repeat step 4 until there is a parent node that represents each symbol and has probability of occurrence 1.
   - Label each node so that the left branches are labeled 0 and the right branches labeled 1.
   - The label on each sheet corresponds to the symbol in which the sheet represents.

   With this algorithm, the less frequent symbols will correspond to the relatively longer encodings and the more frequent symbols will correspond to the relatively shorter symbols. This also ensures that no code is a prefix of any other code, eliminating any ambiguity. See Figure 3 for an example.

- Huffman coding for digital images, Digital image compression using Huffman encoding is similar to using Huffman coding for text file compression. A major difference is that in a digital image, there are a few bytes at the beginning of the file that serve as the file header.
  This file header contains information about the file itself. It describes how bits are used to encode information in digital storage. This file header can not be modified, so the compression process ignores this section.
  The next section is the file itself. This section is of variable size. It can also be modified. However, if a special change is made, such as changing the binary representation, a new file header indicating how to read the file is necessary. Therefore, a new file format may be needed to store this new compressed file.

B. Cryptography

The most common security feature today is cryptography, which is the science of secret code writing [2]. Cryptography is composed of two processes: encryption and decryption. To be effective, this security function must meet the following requirements: Confidentiality, Authentication, Integrity, and Non-repudiation.

1) Chaos based cryptography: In recent years, the transmission of a large amount of data on communication media, such as computer networks, mobile phones, cable TV, etc. was highly developed, making it a security issue in the storage and transmission of confidential information, etc. As a result, research in this area is increasingly important to provide solutions for pay TV, video conferencing, medical and military databases, etc. Most conventional secure ciphers such as: Data Encryption Standard (DES), International Data Encryption Algorithm (IDEA), Advanced Encryption Standard (AES), Linear Feedback Shift Register (LFSR), [3] consider plaintext either as encryption by block or data stream and are not suitable for fast encryption of a large volume of data (eg, color and video images) in real time. Their implementation, when done by the software, of traditional image encryption algorithm is even more complicated because of the strong correlation between the pixels of the image. So, there is still a lot of work to be done for the development of non-traditional encryption methods.

Many researchers have pointed out the existence of a strong relationship between chaos and cryptography. In fact, in real systems, chaos and noise are two irregular behaviors, therefore, the use of these motions in cryptography is also natural. The biggest advantage of a chaotic system is that the system is deterministic, so that the exact knowledge of the initial conditions and system parameters can retrieve a message. This chaos property greatly facilitates the decryption process.

2) The benefits of chaos cryptography: Chaotic systems spontaneously appear in nature and can be applied directly to security processes. Chaos cryptography has several advantages over traditional ones [4]:

- It provides a large assortment of chaotic functions and parameters to be used, thus diversifying the ways that the message can be encoded and increasing of key greatness too.
- In contrast, traditional cryptosystems employ algorithms where scattering and confusion are linear functions of the number of iterations and key lengths.
- As stated in many articles, chaotic mapping functions are randomly without losing their deterministic properties, and an encryption algorithm prevents any statistical analysis from revealing the spectral characteristics of an encrypted signal.

- Chaotic analog cryptography can be directly executed in hardware without having to resort to digital to analog conversion, as traditionally done. As any form of conversion involves a loss of precision and slows down the encryption process, building in a chaotic function continues.
- Chaotic systems have the advantage of being executed with simple quantifiable deterministic algorithms. Thus, chaos provides an alternative to conventional cryptosystem to ensure information security in the open network.

Table I
COMPARISONS OF CHAOS AND CRYPTOGRAPHY.

Chaotic characteristic	Cryptographic property	Description
Ergodicity topological mixing property	Confusion	The output of the system is similar for any input.
Sensitivity to initial conditions and control parametrs	Diffusion	A small difference for the input produce very diffrent output
Deterministic	Deterministic pseudo-randmness	A deterministic procedure produces pseudo-randmness
Complexity	Algorithmic complexity	A simple algorithm produces very complex output

3) The chaos in cryptography: The two basic properties of a good ciphering algorithm, confusion and diffusion, are closely related to the fundamental characteristics of chaos, which are presented in Shannon's work [5], it is clear that the ergodicity properties, self-Similarity, topological mixing are directly related to confusion. On the other hand, diffusion is closely related to the sensitivity of the presented chaotic systems to initial conditions and control parameters. Diffusion produces the avalanche effect, hence a minimal difference in the input of the cryptosystem gives a completely different output. Table I is obtained from Alvarez [6], which summarizes the connection between chaos and cryptography.

4) Chaotic systems: Chaotic cryptography describes the use of chaos theory to perform different tasks in a cryptographic system. Works [7, 8] mark the beginning of chaotic cryptography. Subsequently, the application of chaotic systems to cryptography followed two main approaches: analogue techniques [9] and digital techniques [10]. Analog base cryptosystems use continuous time systems to generate signals for secure communication over a noisy channel, and are based on the synchronization technique [11, 12]. Several systems have been developed that make it possible to transform the information signal into a chaotic waveform on the transmitter side and to extract the information signal from the transmitted wave on the receiver side. The most important among them are: chaotic chaos, shift keying chaos, and chaotic modulation. The basic digital cryptosystems are not based on the synchronization technique, it uses one or more chaotic cards for the encryption of digital data.

Among the various digital base cryptosystems, we can distinguish between the cryptography based on discrete systems (iterative maps) [13], the continuous systems (modeled by differential equations) [14] and combines algorithms using jointly discrete and continuous systems [15]. In this work, we limit our research to the first class of chaotic cryptosystems. Even if they do not display the generic behavior from a physical point of view, these systems are intrinsically interesting: they confirm the main assertion that dynamic instability is the root of irreversibility [16]. In addition, chaotic cryptography from iterative maps is simple and fast.

There are many chaotic systems commonly used in cryptography. Such as the Lorenz System, Logistics Map and the Hénon Attractor. They can be defined using continuous or discrete time scales. Continuous maps are a set of differential equations; While discrete maps are defined as recursive functions. Chaotic cards can also represent any number of dimensions; While continuous systems can only be chaotic with three or more dimensions. Some typical examples are listed as follows:

1) The Lorenz System : is a nonlinear continuous time system with chaotic trajectories for specific values of system parameters as follows :
$$\begin{cases} \frac{dx}{dt} &= \sigma(y-x) \\ \frac{dy}{dt} &= Rx - y - xz \\ \frac{dz}{dt} &= xy - z\beta \end{cases}$$
Where σ, R, β are the system parameters.
2) Logistics map : the well-known logistics function is$x_{n+1} = rx_n(1-x_n)$, $x \in [0,1]$
The logistic map is a well-known one-dimensional map showing behavior chaotic for the values of the parameter r on the interval (3.56995 - 4). However, it is important to note that for some values of r over this interval, we can also show what is non-chaotic.
3) The attractor of Hénon [17]: is a dynamic system with discrete time. It is one of the most studied dynamical systems with chaotic behavior
$$\begin{cases} x_{n+1} = y_n + 1 - ax_n^2 \\ y_{n+1} = bx_n \end{cases}$$
It depends on two parameters, a and b, which have canonical values: a = 1.4 and b = 0.3. For these values, the attractor of Hénon is chaotic. For other values of a and b, it can be chaotic, intermittent or converge to a periodic orbit. As a dynamic system, Henon's canonical attractor is of particular interest because, unlike the logistic map, his orbits do not have a simple description

Obviously, there are still many other chaotic systems, which will not be listed here. Readers can refer [18, 19] for more details.

C. styganography

The word steganography comes from two Greek words, steganos meaning "hidden" or "protected" and graphein meaning "writing". According to the definition of D. Kundur and K. Ahsan [20], steganography is the secretive hiding of data

in a given host carrier for the purpose of improving value or exchanging information in a covert manner.

The host carrier is a message of some kind that contains redundancy or irrelevance. For example, digital image files are often used to embed secret information; Limiting human vision by noticing subtle differences between hues can hide data from this type of media. Primarily, it is of three categories [21]: (i) steganography in the image, (ii) steganography in audio / video, and (iii) protocol steganography. In recent literature steganography work in text has also been proposed [22].

In image steganography the secret message is hidden inside an image in such a way that the change in the quality of the image can not be noticed. In the Audio / Video Steganography the secret message is hidden in an audio file like a song or music without changing or disrupting the original quality of it. In protocol steganography, the secret message is embedded in the network control protocols used for transmission, in the layers of the OSI network model, there are secret routes where steganography can be used, for example the header of a TCP / IP packet [23].

According to [24], steganography has three important measures: capacity, imperceptibility and robustness.

Capacity is the maximum size of secret information that can be embedded in a file. As explained in [24], " The capacity can be defined as an absolute value in terms of number of bits for a particular coverage or as a relative number with respect to the bits needed to save the final stego file ". The value of the capacity depends on the integration function and the properties of the cover.

An image of stego should not have any significant perceptual artefact, hence the imperceptibility . The higher the fidelity of the stego image, the more imperceptible it is. This is to mention that the stego image and the original image need not be distinguishable.

Robustness is the property of the harness to eliminate secret information from the stego image. In other words, it is the resistance level of the stego image when it is intentionally distorted by another party. The robustness metrics of steganographic algorithms have distortion classifications such as geometric transformations or additive noise [24].

1) Steganography on Digital Images: This work will focus on hiding information in pictures. Thus, image steganography techniques can be classified into two broad areas such as space domain and frequency domain (transformed) domain techniques [21] as shown in Figure 4. In space domain techniques the secret message is hidden in the image by applying some manipulation on the different pixels of the image. In frequency domain techniques, the image is transformed to another form by applying a transform as a discrete wavelet transform, and then the message is hidden by the application of one of the usual embedding techniques. Each domain is further classified into different techniques according to their actual implementation. For example the most known spatial domain techniques are (I) LSB, (ii) Pseudo-random LSB, (iii) PVD, and the best-known techniques are frequency domain : (i) DCT, (ii) DWT, (iii) DFT.

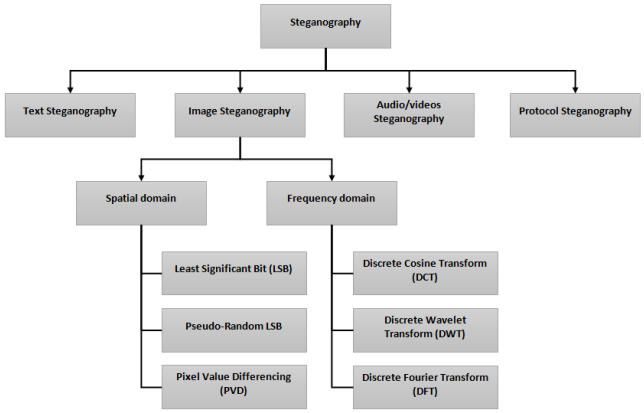


Figure 4. Classification of Steganography techniques

2) Space Domain Techniques:

a) LSB Technique : This is one of the most common and easiest methods for the message hiding. In this method, the message is hidden in the least significant bits of the image pixels. Changing the LSB of the pixels does not present much difference in the image and therefore the image of stego resembles the original image. In the case of 24 bit image three pixel bits can be used for LSB change since each pixel has separate components for red, green and blue. In other words, we can store 3 bits in each pixel. An image of 800 x 600 pixels, can thus store a total amount of 1 440 000 bits or 180 000 bytes of the embedded data [25].:

- Advantage
  - The quality of the cover image is barely touched.
  - Good concealment ability.
  - Very simple in the implementation
- Disadvantage
  - Detection of secret data is easy because of simplicity of algorithm.
  - Robustness is weak.
  - Storing more information requires a large image size.

b) Pseudo-random encoding technique LSB: In this technique, a random key is used to choose random pixels where the bits of the message are saved. This will make the message bits harder to find for an intruder. In addition, the colorful three-plane (RGB) image. Data can be hidden in the LSB of any color plane of randomly selected pixels [26]. With the use of this technique, it will be difficult for the attacker to identify the schema in which the message bits are hidden, as no particular pattern applies for embedding the bits of the subsequent message.:

- Advantage
  - Degradation of the cover image will be very small because the identified pixels are distant from each other.
  - The ability to incorporate is good.
  - Simple to implement.
- Disadvantage

- Access to the key, can easily detect the location of pixels in the image cover and so easily reveal the secret message.
- More information storage requires a large image size, which requires a high transmission rate because of the stego image size.

c) Pixel Differential Value (PVD) Technique : Based on the fact that our human vision is sensitive to slight changes in the smooth regions, while can tolerate more severe changes in the edge regions, PVD-based methods have been proposed to improve the integration capability without introduce obvious visual artifacts into stego images. In PVD-based schemes, the number of embedded bits is determined by the difference between the pixel and its neighbor. The greater the amount of difference, the more secret bits can be incorporated. Usually, PVD-based approaches can achieve more imperceptible results compared to these typical LSB-based approaches with the same integration capability.:

- Advantage
  - Works better than LSB that directly embed secret data regardless of the difference between the two pixels.
  - Stego images produced are very similar to the original image.
- Disadvantage
  - Considerable distortion of the stego image can occur when the PVD method adjusts the two consecutive pixels in order to hide the secret data in the value of the difference.
  - A boundary problem can occur when the two consecutive pixels are located in the end of the width or smooth areas or when the values of two consecutive pixels form a contrast.

3) Frequency domain techniques:

a) Discrete cosine transform (DCT) technique: In this technique, the image is converted into a frequency domain [27]. This transformation process is divided into four distinct and independent phases. (i) In this phase, the image is divided into 8 x 8 pixel size blocks. (ii) Each block is DCT transformed to convert the information in the frequency domain . (iii) Phase 1 information is quantified to remove superfluous information in the frequency domain. (v) Technical Standard Compression will be applied to the binary model [28]. This transformation is mainly used when the stego image is subject to image editing processes such as compression, cropping, and so on. This explains the reason for storing data in the image domains, which are not much affected after the application of these processes.:

- Advantage
  - Very robust, since the cover image is transformed before storing data.
  - Even after applying the image editing processes the data remains safe.
  - Less bandwidth required for image-stego transmission because its size can be reduced.
- Disadvantage
  - Only a few secret messages can be incorporated in the cover image, to the reason that the data should only be stored in the transformed image.
  - Image quality is very degraded which gives information about the presence of the message in the cover image.

b) Discrete wavelet transform technique (DWT) : is another frequency domain transformation proposed by [29]. This technique is divided into two operations , horizontal operation and vertical operation. The different stages of the procedure are as follows: :

1) Step 1: The pixels in a line are analyzed from left to right and addition and subtraction operations are performed on neighboring pixels. On the left side the sum of the pixels is stored and on the right side the difference in value is stored. This process is repeated for all lines. The pixel addition gives the low frequency components and the pixel difference gives the high frequency components of the original image.
2) Step 2 : The pixels are scanned in the vertical direction column from top to bottom. The sum and the difference are calculated on the neighboring pixels. The summation of pixels in the column is stored at the top and difference value is stored in the lower part. This process is repeated for all columns. The information is converted into four sub-bands described as LL, HL, LH and HH. The LL sub-band looks a lot like the original image, as it is the low frequency part [29].

- Advantage
  - Very robust, since the cover image is transformed before storing data.
  - Even after the application of certain processing and image signal noise the data remains safe.
  - The capacity of incorporation is very high.
- Disadvantage
  - Complexity of this technique is high.
  - The speed is slower because of the long procedure.

c) Discrete Fourier Transform (DFT) technique: This technique is similar to the DCT technique, but it uses the Fourier transform instead of the cosine which makes it not resistant to strong geometric distortions. Although it increases the overall complexity of the process. :

- Advantage
  - Very robust : Even after applying certain image processing changes, the data remains safe.
  - A less need for bandwidth for image-stego transmission because its size can be reduced.

  Disadvantage
  - The complexity of this technique is very high.
  - Only a few secret messages can be incorporated into the cover image.
  - Low storage capacity, compared to other techniques.

Table II
A GLOBAL COMPARISON BETWEEN STEGANOGRAPHY TECHNIQUES.

Parametres	LSB	LSB P-R	PVD	DCT	DWT	DFT
Imperceptibility	1	1	1	5	5	5
Robustness	2	2	2	4	5	5
Security	6	3	3	2	1	1
Efficiency	2	2	2	3	4	5
Capacity	2	2	3	4	3	4

4) Overall comparison between steganography techniques: Table. II presented an overall comparison between the different steganography image techniques previously described, by reference to the performance measurement parameters that are present in section **??**. The results of this comparison are obtained based on the simulations presented in [30], where 1 to 6 indicates, strong to low performance. (1) very good, (2) good, (3 and 4) Average, (5) above average and (6) weak.

1) The visual quality of stego-image produced by space-domain techniques is better than that produced by frequency-domain techniques.
2) Frequency domain techniques are less sensitive to small changes in the image, unlike spatial domain techniques, when applying signal processing methods can fully mix the secret information. This can result in a total loss of information.
3) The time taken by the space domain techniques remained the same for the different image sizes. On the other hand, the temporal complexity of the frequency domain techniques increases with the increase of the image size.
4) The storage capacity of space domain and frequency domain techniques is totally dependent on the size of the coverage image.
5) According to the results presented by different measurements, it is clearly concluded that spatial techniques giving a picture-stego highly correspond to the cover image.

III. MOTIVATION AND CHALLENGES

After a thorough bibliographic search on the three basic terminologies of our study on compression, cryptography and steganography. We are at the point of proposing a new hybrid system method that is based on a combination of an innovative encryption method and a better steganography method, this proposal must ensure the following three objectives:

- The perceptual quality of the image should be high.
- The complexity of time should be low.
- Inclusiveness should be high.

IV. OUR PROPOSAL :

In this section we will represent our proposal which presents the general security model of the proposed hybrid technique. As shown in Figure 5. The proposed new model compresses the data first. The purpose of this compression step is to reduce the size of the data to be transmitted in order to increase the amount of data to be masked in the cover image as well as to improve the level of security. The next step is to encrypt the compressed message using chaos theory-based encryption. In this step, a chaotic system is integrated which makes it possible to secure the positions of the pixels concerned by the insertion.

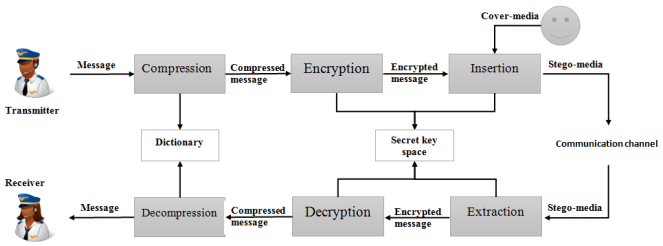


Figure 5. General model of hybrid security proposed.

Indeed, unlike existing methods where the integration of secret message is sequentially from top to bottom, and from left to right, the chaotic system chooses in an almost chaotic manner the positions of the pixels involved in the insertion. With this novelty the system security will be increased and the complexity of the time will be diminished. The final step is to use Steganography to insert the message content into the cover image. In this work we choose to use a spatial technique of Steganography. The reverse process is performed on the receiver side as also shown in Figure 5.

V. CONCLUSION

Based on an introduction to the different terminologies used in our work and a state of the art on each technology. So, in this paper, we propose a new hybrid technique, which has increased the layers of security in the overall system. With the use of Huffman compression, chaos-based cryptography and Steganography's LSB technique. Combining these three techniques into a single security system will not only be robust and more efficient, but its integration capacity will also increase and the complexity of time will be minimal compared to other available techniques. The next work is the implementation and validation of our proposal.

REFERENCES

[1] G. P. Pratishtha Gupta and V. Bansal, "A survey on image compression techniques," *in International Journal of Advanced Research in Computer and Communication Engineering*, vol. 3, no. 8, pp. 7762–7768, 2014.

[2] R. Nivedhitha and D. T.Meyyappan, "Image security using steganography and cryptographic techniques," *International Journal of Engineering Trends and Technology*, vol. 3, no. 3, pp. 366–371, 2012.

[3] F. P. Miller, A. F. Vandome, and J. McBrewster, *Advanced Encryption Standard*. Alpha Press, 2009.

[4] A. Pisarchik and M. Zanin, "Image encryption with chaotically coupled chaotic maps," *Physica D: Nonlinear Phenomena*, vol. 237, no. 20, pp. 2638 – 2648, 2008.

[5] C. Shannon, "Communication theory of secrecy systems," *Bell System*, vol. 28, 1949.

[6] E. Alvarez, A. Fernandez, P. Garcıa, J. Jiménez, and A. Marcano, "New approach to chaotic encryption," *Physics Letters A*, vol. 263, no. 4, pp. 373–375, 1999.

[7] R. Matthews, "On the derivation of a chaotic encryption algorithm," *Cryptologia*, vol. 8, no. 1, pp. 29–41, jan 1984.

[8] L. M. Pecora and T. L. Carroll, "Synchronization in chaotic systems," *Phys. Rev. Lett.*, vol. 64, pp. 821–824, Feb 1990.

[9] J. Liu and L. Tsimring, *Digital Communications Using Chaos and Nonlinear Dynamics*, ser. Institute for Nonlinear Science. Springer New York, 2006. [Online]. Available: https://books.google.dz/books?id=4ehFAAAAQBAJ

[10] J. Awrejcewicz, *Bifurcation and Chaos: Theory and Applications*, 1st ed. Springer Publishing Company, Incorporated, 2012.

[11] L. M. Pecora and T. L. Carroll, "Synchronization of chaotic systems," *Chaos: An Interdisciplinary Journal of Nonlinear Science*, vol. 25, no. 9, p. 097611, 2015.

[12] L. KOCAREV, K. S. HALLE, K. ECKERT, L. O. CHUA, and U. PARLITZ, "Experimental demonstration of secure communications via chaotic synchronization," *International Journal of Bifurcation and Chaos*, vol. 02, no. 03, pp. 709–713, 1992.

[13] M. Mishra and V. H. Mankar, "Chaotic encryption scheme using 1-d chaotic map," *CoRR*, vol. abs/1312.4042, 2013.

[14] T.-I. Chien and T.-L. Liao, "Design of secure digital communication systems using chaotic modulation, cryptography and chaotic synchronization," *Chaos, Solitons, Fractals*, vol. 24, no. 1, pp. 241 – 255, 2005.

[15] D. Xiao, X. Liao, and P. Wei, "Analysis and improvement of a chaos-based image encryption algorithm," *Chaos, Solitons, Fractals*, vol. 40, no. 5, pp. 2191 – 2199, 2009.

[16] N. Masuda, G. Jakimoski, K. Aihara, and L. Kocarev, "Chaotic block ciphers: from theory to practical algorithms," *IEEE Transactions on Circuits and Systems I: Regular Papers*, vol. 53, no. 6, pp. 1341–1352, June 2006.

[17] M. Hénon, "A two-dimensional mapping with a strange attractor," in *The Theory of Chaotic Attractors*. Springer, 1976, pp. 94–102.

[18] A. N. Pisarchik and M. Zanin, "Chaotic map cryptography and security," *International Journal of Computer Research*, vol. 19, no. 1, p. 49, 2012.

[19] L. Kocarev and S. Lian, *Chaos-based cryptography: Theory, algorithms and applications*. Springer, 2011, vol. 354.

[20] D. Kundur and K. Ahsan, "Practical internet steganography: Data hiding in ip," 04 2003.

[21] A. Cheddad, J. Condell, K. Curran, and P. Mc Kevitt, "Review: Digital image steganography: Survey and analysis of current methods," *Signal Process.*, vol. 90, no. 3, pp. 727–752, Mar. 2010. [Online]. Available: http://dx.doi.org/10.1016/j.sigpro.2009.08.010

[22] kamaldeep, "Image steganography techniques in spatial domain, their parameters and analytical techniques: a review article," vol. 2, no. 5, pp. 85–92, 2013.

[23] K. Curran, J. Condell, P. M. Kevitt, and A. Cheddad, "Enhancing steganography in digital images," in *2008 Canadian Conference on Computer and Robot Vision(CRV)*, vol. 00, 05 2008, pp. 326–332.

[24] A. A. J. Altaay, S. B. Sahib, and M. Zamani, "An introduction to image steganography techniques," in *Proceedings of the 2012 International Conference on Advanced Computer Science Applications and Technologies*, ser. ACSAT '12. IEEE Computer Society, 2012, pp. 122–126.

[25] Y. K. Lee and L. H. Chen, "High capacity image steganographic model," *IEE Proceedings - Vision, Image and Signal Processing*, vol. 147, no. 3, pp. 288–294, June 2000.

[26] J. Hossain, "Information-hiding using image steganography with pseudorandom permutation," *Bangladesh Research Publication Journal*, vol. 9, no. 3, pp. 215–225, 2014.

[27] M. Tayel and H. Shawky, "A proposed assessment metrics for image steganography," *International Journal on Cryptography and Information Security (IJCIS)*, vol. 4, no. 1, 2014.

[28] H. Sheisi, J. Mesgarian, and M. Rahmani, "Steganography: Dct coefficient replacement method andcompare with jsteg algorithm," *International Journal of Computer and Electrical Engineering*, vol. 4, no. 4, p. 458, 2012.

[29] P.-Y. Chen, H.-J. Lin *et al.*, "A dwt based approach for image steganography," *International Journal of Applied Science and Engineering*, vol. 4, no. 3, pp. 275–290, 2006.

[30] S. Dhall, B. Bhushan, and S. Gupta, "An in-depth analysis of various steganography techniques," *International Journal of Security and Its Applications*, vol. 9, no. 8, pp. 67–94, 2015.

Face Identification using Kinect Depth-Maps under One Sample per Person Scenario

Ahmed Yassine Boumedine*, Samia Bentaieb† and ‡ Abdelaziz Ouamri
Laboratory Signals and Images LSI, USTO-MB, B.P. 1505 El Mnaouer, Oran, Algeria
Email: *ahmdiassine@gmail.com, † bentaiebsamia01@yahoo.fr, ‡ ouamri@yahoo.com

***Abstract*—In this paper, we present a matching approach in a process of face recognition based on SURF descriptor, for noisy low resolution 3D faces acquired by Kinect sensor under One Sample per Person Scenario. After the detection of the nose tip, the face is extracted and centered around it's nose tip, then the noise is removes using mean filter. The SURF algorithm is applied on the shape index map to find interest points and their descriptors used to construct a dictionary using only one sample per person. In the identification process, the SSD is used to find the best match between the SURF descriptors extracted from a probe face and the dictionary. Experiments have been performed on CurtinFaces dataset. Identification accuracy achieved rank one recognition rates of 94.38% and 71.15% for the neutral and smiling expression respectively.**

***Index Terms*—face recognition, Kinect, SURF, shape index**

I. Introduction

With it non-intrusiveness property, face recognition has become an important technology in computer vision especially with the growing need for reliable identification/ authentication and access control systems. In recent years, identification of face images acquired in an uncontrolled environment has received large amount of attentions from the biometrics research community. It may be done on a face represented by a two-dimensional (2D) intensity image. Nevertheless, this has some limitations, such as facial expressions and partial occlusions and its high sensitivity to pose and illumination variations. In addition to these problems, having one sample per person (OSPP) is a significant challenge for an identification/ authentication system in real-world situations, since only one scan is stored in the gallery while a high variability of facial appearances of that same subject may exist.

With the development of three-dimensional (3D) imaging technology, 3D FR is expected to overcome the limitations of 2D systems. Using the shape of the face and depth information, rather than color information, is effective and robust in different conditions, such as pose variations and changes in lighting conditions. Major inconveniences of existing 3D scanners that can capture high resolution 3D data are generally their slowness and expensive cost. Nowadays, with the recent success of low cost and high speed RGB-D cameras, such as the Microsoft Kinect devices, the depth information has become easily acquirable and useful for face recognition. A comparison between faces images with Minolta VIVID 910 scanner (top) against Kinect (low) is provided in Fig. 1

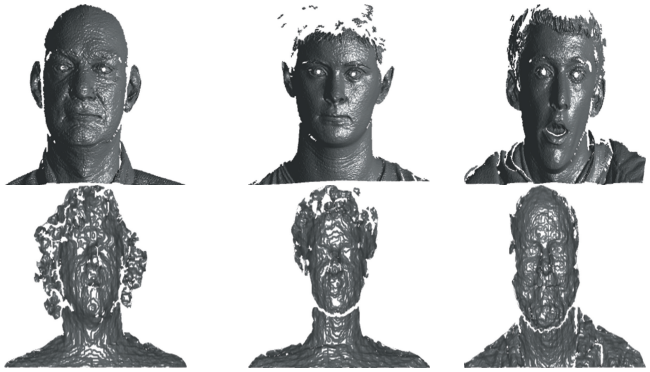


Fig. 1: 3D scans from FRGC dataset [1] acquired with Minolta and Kinect sensors: top row: 3D faces from FRGC dataset, low row: 3D faces from Curtinface dataset [2].

II. Related Work

To overcome these challenges, several approaches have been proposed and discussed the use of using RGB-D data captured from the Kinect sensors. In [3], a continuous 3D face authentication system that uses a RGB-D camera is proposed. After face detection and normalization using ICP algorithm, each facial image is divided in three different Regions of Interest (ROI): the left half of the face, the nose region and the right half of the face. HoG features are extracted and matched to corresponding ROI. Evaluated on four 40 minutes long videos with variations in facial expression, occlusion and pose, an Equal Error Rate (EER) of 0.8% is achieved. Note that the color information is ignored in order to avoid the limitations of pose and illumination variations.

Li et al. [2] proposed a preprocessing algorithm which exploits the facial symmetry at the 3D point cloud level to obtain a canonical frontal view for shape and texture faces irrespective of their initial pose. First, each gallery face faces is registered to a reference model then facial symmetry is employed to fill holes and smooth the face depth data. Finally, Sparse Representation Classifier (SRC) is used for both depth and texture separately. The approach is tested CurtinFaces dataset and achieved 88.7% of recognition rate using depth data only and 96.7% when face texture and depth are fused.

Ciaccio et al. [4] proposed an approach robust to head rotations using a single gallery RGB-D face images while the probes can be at any pose angle. The face is first detected from the RGB image then noise removal and smoothing of

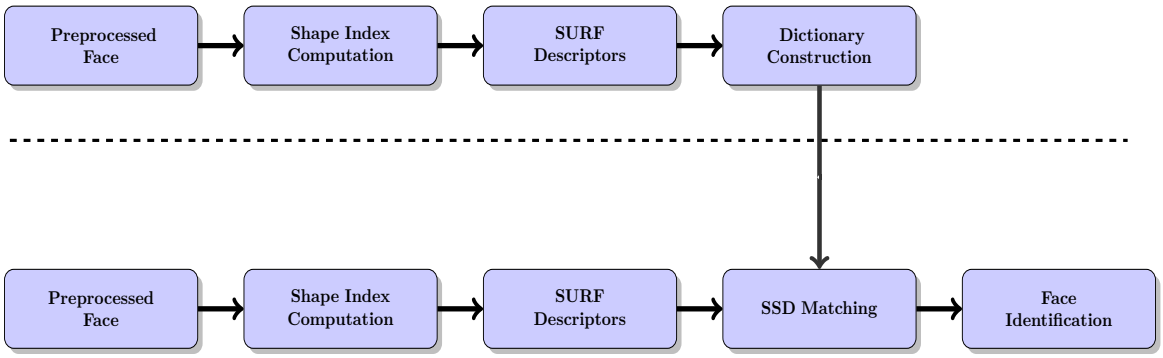


Fig. 2: Diagram of the proposed approach

the depth map are performed using a median filter followed by a Gaussian filter. For recognition, a new face representation that combines the covariance descriptor with the LBP features is presented. Experiments conducted on CurtinFaces dataset showed that better results are achieved when combining LBP and covariance descriptor.

Goswami et al. proposed in [5] a Kinect-based face recognition algorithm that computes a descriptor based on the entropy of RGB-D faces along with the saliency feature obtained from a 2D face. Concatenation of five HOG descriptors is used as input to the trained Random Decision Forest (RDF) classifier for establishing the identity of a probe RGB-D face.

In [6], the authors presented a fusion of two approaches: RGB-D Image descriptor based on Saliency and Entropy (RISE) and Attributes based on Depth Map (ADM) combined for face recognition. RISE algorithm used a combination of entropy, visual saliency, and depth information with HOG for feature extraction and RDF for classification while Further, the ADM algorithm is performed to extract and match geometric attributes. ADM is then combined with the RISE algorithm for identification. In [7], the authors have assessed the fusion of 3DLBP with the Histogram of Averaged Oriented Gradients (HAOG), a variant of HOG (Histogram of Oriented Gradients) for face recognition on Kinect depth maps. Boutella et al . [8] explored the usefulness of four local feature extraction methods (LBP, LPQ, HOG and BSIF) for both face texture and shape applied to identity, gender, and ethnicity recognition task. Azakhnini et al. [9] studied which facial parts are most effective for learning gender, ethnicity and emotional state based on RGB-D information.

SURF feature has been successfully investigated as a descriptor for 2D face recognition [10], [11], nevertheless it has not been addressed in 3D face recognition as well as SIFT. Only a few studies have been proposed based on SURF feature. In [12], authors proposed a two-stage procedure of 3D face recognition based on depth image and SURF. First, they used Fisher Linear Discriminant (FLD) method on the depth image to perform coarse recognition. Then, they extracted the SURF features of the 2D gray images, that are corresponding only to the highly ranked 3D faces, to carry out the refined recognition. Ajmera et al [13] proposed the use of SURF descriptors in Kinect scans. Images with variation in pose are generated, and SURF is also used for face matching independently on depth and intensity images. Bentaieb et al. [14] proposed and evaluated a three-dimensional (3D) face recognition approach that applies the speed-ed up robust feature (SURF) algorithm to the depth representation of shape index map, under real world conditions, using only a single gallery sample for each subject. First, the 3D scans are preprocessed, then SURF is applied on the shape index map to find interest points and their descriptors. Each 3D face scan is represented by keypoints descriptors, and a large dictionary is built from all the gallery descriptors. At the recognition step, descriptors of a probe face scan are sparsely represented by the dictionary.

III. PROPOSED APPROACH

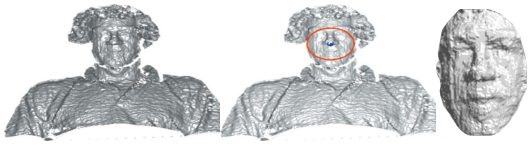
We propose and evaluate a three-dimensional (3D) face recognition approach, described in Fig. 2, that applies the Speeded Up Robust Feature (SURF) algorithm to the depth representation of shape index map using only a single gallery sample for each subject. First, the 3D scans are preprocessed, then SURF is applied on the shape index map to find interest points and their descriptors. Each 3D face scan is represented by keypoints descriptors, and a large dictionary is built from all the gallery descriptors. The proposed approach relies only on the depth maps and do not use the RGB images. In the following subsections, we describe these phases in detail.

A. *Preprocessing*

3D data are visibly imperfect and usually contain noise that will significantly affect the following preprocessing and feature extraction steps. Furthermore, scans contain not only the face but additional parts like the neck, the shoulders, the chest and clothes as Fig. 3a clearly shows .

First the nose tip is detected assuming that it is the closest point to the camera in cases of dealing with frontal pose only.

A sphere of radius $90mm$ (see Fig. 3b) centered at the nose tip is then used to crop the 3D face and discard other captured regions as illustrated in Fig 3c.



(a) (b) (c)

Fig. 3: (a) sample from CurtinFaces dataset, (b) face cropping using a sphere of radius $90mm$ around the nose tip , (c) the cropped face.

Denoising is a very important part of the process, especially when dealing with 3D maps taken from a Kinect sensor. The most popular technique for removing noise is the mean filter. This technique consists of examining a small neighbourhood of each point and replacing its depth with the mean depth of the points in that neighbourhood. Fig. 4 shows facial surface that contains noise and it denoised version ready to be used for the recognition.

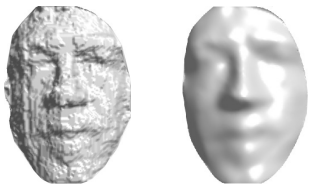


Fig. 4: Face denoising: (a) facial surface, (b) denoised facial surface.

B. Shape Index Computation

The curvature is a second differential property that measures how the direction of the surface normal changes along the surface. It has been widely used in facial feature detection [15], [16] and face recognition [17]–[19] . The extraction of the principal curvatures is one of the most common methods for characterizing a 3D surface.

Given a 3D facial surface S, a curve is formed by the intersection of the surface and the normal plane in a tangent direction t at a point P. The curvature of this planar curve is the normal curvature κ_n. Rotating the normal plane will yield to different curvatures; the maximum value and the minimum value of these curvatures form the principal curvatures and are denoted κ_1 and κ_2, respectively.

Based on the idea that the geometry of a smooth surface S can be locally approximated using a quadratic polynomial surface, we locally fit a smooth quadratic surface and compute easily the differential quantities. The principal curvatures are computed by first rotating the local neighborhood points in radius r_{dist} around a point P so that the normal of the current point is aligned with the Z-axis, then, a least-square quadratic patch [20]:

$$f(x,y) = Ax^2 + By^2 + Cxy + Dx + Ey + F, \quad (1)$$

is fitted to the local neighborhood of P and the eigenvectors and eigenvalues of the Hessian matrix are used to calculate the principal curvatures.

The Shape Index (SI) as proposed by Koenderink et al. [21] describes surface attributes of shapes. The shape index value at point P is defined as:

$$SI(P) = \frac{1}{2} - \frac{1}{\pi} \arctan \frac{\kappa_1(P) + \kappa_2(P)}{\kappa_1(P) - \kappa_2(P)}, \quad (2)$$

As the principal curvatures are invariant to translation, rotation and scale so is the shape index. The shape index lies in the interval $[0,1]$ and describes regions of a surface ranging from spherical cup when $SI(P) = 0$ to spherical cap when $SI(P) = 1$.

The parameter r_{dist} is quite important for the process. If its value is too small, the curvature value will be local, and the map will not be representative enough for the shape analysis. If its value is too big, a great part of the details will be lost. In this paper, this parameter is set to 15 mm.

Once the shape index is computed for every point of the facial surface, it is mapped into a range image as shown in Fig. 5.

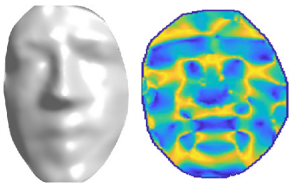


Fig. 5: An illustration of the shape index map of 3D facial surface.

C. SURF Feature Selection

Given a shape index range image, we apply the SURF algorithm [22] to detect significant points. For a point $X = (x, y)$ in a range image I, the Hessian matrix at scale σ is defined as:

$$H(X,\sigma) = \begin{bmatrix} L_{xx}(X,\sigma) & L_{xy}(X,\sigma) \\ L_{xy}(X,\sigma) & L_{yy}(X,\sigma) \end{bmatrix}, \quad (3)$$

where $L_{xx}(X,\sigma)$, $L_{xy}(X,\sigma)$ and $L_{yy}(X,\sigma)$ are respectively, the convolution of the Gaussian second-order derivatives with the image I at the point X. Box filters are used to approximate the second-order Gaussian derivatives. Image convolutions with box filters are computed rapidly using integral images.

The determinant of the Hessian matrix is calculated for detecting the extremum points in scale space. A threshold is applied to decide which point is considered as a keypoint. The higher the threshold, the less keypoints are detected. In this paper, the threshold is set to 0 in order to take more keypoints.

To generate the descriptors, a square region is constructed around each point of interest and aligned along the dominant direction. This square region is then divided into 16 subregions of size 4×4. For each of these subregions, Haar wavelet

responses are calculated. The responses and their absolute values are summed up over each subregion and form the descriptor vector Descr:

$$Descr = \left\{ \sum dx, \sum dy, \sum |dx|, \sum |dy| \right\}, \tag{4}$$

Thus, the SURF descriptor vector of a keypoint is formed by applying the above process to all of the sixteen subregions and concatenating their descriptor vectors to get a descriptor vector of length 64.

D. Face Identification

1) Gallery Dictionary Construction: We construct the gallery dictionary of keypoint descriptors as follows. Suppose that the gallery contains C subjects and for c^{th} subjects, k_c SURF keypoints are detected. Their corresponding 64-dimensional local descriptors, denoted $D_{c1}, D_{c2}, ...D_{ck_c}$, are computed and concatenated to build the gallery sub-dictionary of the subject c as:

$$D_c = [D_{c1}, D_{c2}, ...D_{ck_c}], \tag{5}$$

The sub-dictionaries of all the C subjects are built in the same manner and gathered to construct the gallery dictionary:

$$D = [D_1, D_2, ...D_C] \in \mathbb{R}^{64 \times K}, \tag{6}$$

where $K = k_1 + k_2 + ...k_C$ represents the total number of keypoint descriptors in the gallery dictionary.

2) SSD-based Face Recognition: Let Y represent the n keypoint descriptors, detected for a probe face:

$$Y = (y_1, y_2, ..., y_n), \tag{7}$$

The recognition problem is formulated as a Sum of Squared Difference (SSD) problem as follows. Each descriptor y_i of the probe face is compared to all D_j descriptors of the gallery set. Let $E_i(j)$ represents the SSD value between D_j and Y_i

$$\begin{gathered} E_i(j) = \sum_{k=1}^{64} [D_{k,j} - Y_{k,i}]^2 \in \mathbb{R}^{1 \times K}, \\ i = 1, 2, ..., n,\ j = 1, 2, ..., K, \end{gathered} \tag{8}$$

Denote $X \in \mathbb{R}^{1 \times K}$, a test descriptor is the most similar to one descriptor represented in the dictionary. This means that the entries of X are almost zero except the ones where $E_i(j)$ is minimum, Since the descriptors of the probe face are independent from each other, we solve n similar minimization problems.

To determine the identity of the test face, we use:

$$identity(Y) = \underset{c}{argmax} \left\| \delta_c (X) \right\|_0 \tag{9}$$

where $\delta_c(.)$ is the characteristic function which selects the coefficients corresponding to the c^{th} and $\|.\|_0$ denotes the l_0-norm which counts the number of nonzero elements of a given vector.

The class that yields the maximum non-zero entries along all the different classes in the dictionary corresponds to the identity of Y.

Logically, two faces can be considered to be more similar if they have a high number of similar descriptors with a low Euclidean distance between them. To this end, we propose a weight sparse representation method that fuses both sparsity and similarity.

We first compute For each probe descriptor y_i,

$$\begin{gathered} d_i = \sum_{k=1}^{64} [D_{k,j} - Y_{k,i}]^2, \\ i = 1, 2, ..., n,\ \ j = 1, 2, ..., K, \end{gathered} \tag{10}$$

the SSD between y_i and all the descriptors in the dictionary D. Then for each y_i, we preserve only the descriptor according to the top smallest value of d_i denoted by $E_m (1 < m < K)$. The smallest value of d_i over all $i = 1, 2, ..., n$ is denoted by E.

Denote $\widehat{X}$ a sparse vector $\in \mathbb{R}^{1 \times K}$. The entries of $\widehat{X}$ are almost zero except for the top smallest value of d_i where :

$$\widehat{X}(m) = 1 + \frac{E}{E_m} \tag{11}$$

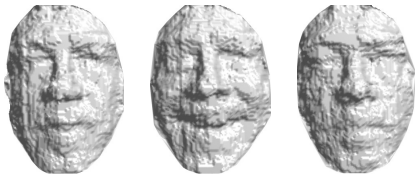
Finally; to determine the identity of the test face, we use:

$$identity(Y) = \underset{c}{argmax} \left\| \delta_c \left(\widehat{X} \right) \right\|_0 \tag{12}$$

IV. Experimental results

The proposed approach is evaluated on the CurtinFaces dataset [2] which contains over 5000 images of 52 subjects in both RGB and depth maps obtained by Kinect sensor. The participants consist of 10 females and 42 males. The subjects in the database belong to three different ethnic groups: Caucasians, Chinese and Indians. The facial images have various variations in pose, illumination, facial expression as well as sunglasses and hand disguise. The faces of each subject are acquired under many combinations of these challenges. For each subject, there are 49 images under 7 poses and 7 facial expressions, 35 images under 5 illuminations and 7 expressions, and 5 images under disguise (sunglasses and hand).

We use one neutral and frontal scan from each subject for training, and two subsets containing images with a frontal pose, smiling expression and high illumination and frontal pose with neutral expression and low illumination as shown in Fig. 6 are used for testing. For face identification, we use the Cumulative Match Characteristic (CMC) curve and the rank-1 identification rate (rank-1 IR) to measure system performance. The CMC plots the identification rate at rank k and rank-1 IR is the percentage of all probes for which the best match in the gallery belongs to the same subject.



(a) (b) (c)

Fig. 6: Gallery and probe for a subject in the CurtinFaces dataset: (a) training sample, (b) and (c) testing sample.

On the subset of frontal pose with neutral expression and low illumination an accuracy of 94.23% is achieved in both cases(with and without weight). On the subset that contains only images with a frontal pose, smiling expression and high illumination, an accuracy of 65.38% is achieved when giving the same weight to each matching and an accuracy of 71.15% when giving different weights. Table I shows rank-1 IRs rates of the proposed approach. It achieves an overall rank-1 IR of 82.69%.

Testing set	without weight	with weight
neutral vs neutral	94.23%	94.23%
neutral vs smile	65.38%	71.15%
neutral vs all	79.80%	82.69%

TABLE I: Rank-1 IRs on different subsets of the CurtinFaces dataset.

Approach	Dataset	Accuracy
Ciaccio et al. 2013 [4]	CurtinFaces	84.6% (RGB-D)
Li et al. 2013 [2]	CurtinFaces	88.7% (D)
Our approach	CurtinFaces	82.69% (D)

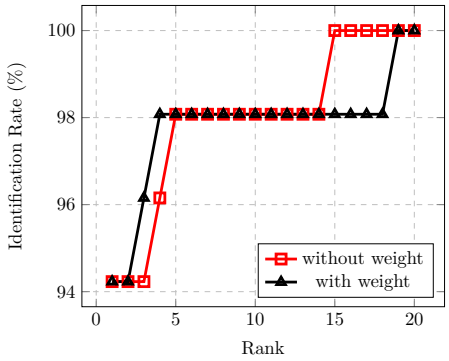
TABLE II: Comparison of rank-1 IRs with the state-of-the-art approaches on the CurtinFaces dataset.

Table II shows a summary of the reported performance usink Kinect sensor. Goswami et al. [6] reported an accuracy of 86% when using one sample per person to test the their approach on RGB-D data and an accuracy of 89% when using 4 samples. Ciaccio et al. [4] achieved an accuracy of 84.6% when using one sample per person of a frontal pose and neutral expression to test the the proposed framework on RGB-D data of different poses and neutral expression. Li et al. [2] had an accuracy of 88.7% when using 18 samples of the depth map for training. Our method outperforms their approach since only one sample need to be used to achieve better performance. The cumulative matching curves are shown in Fig. 7.

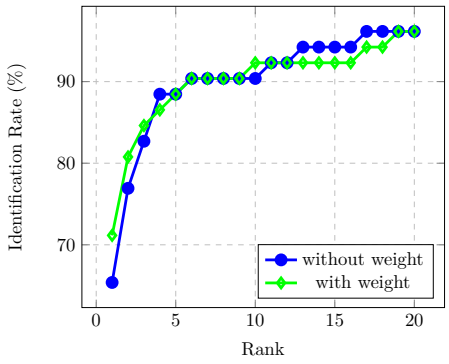
V. Conclusion

In this paper, we proposed an automatic 3D face recognition approach from low quality Kinect acquired data. The proposed approach used SURF on shape index maps to find interest points and their descriptors. In the identification process, the SSD is used to find the best match between the SURF descriptors of a probe face and the dictionary.

The proposed approach relies only on the depth maps (do not use the RGB images) and can effectively handle one sample per person scenario, reaching competitive performances.



a – The CMC curves neutral vs. neutral



b – The CMC curve of neutral vs. smile expression

Fig. 7: CMC curves of the proposed approach.

Identification accuracy achieved rank one recognition rates of 94.38% and 71.15% for the neutral and smiling expression respectively of the CurtinFaces dataset.

For future works, we will explore three aspects: first, our approach will be extended to address FR under pose variations. Second, the features we used are derived from the shape index while multiple differential surface measurements can characterize a facial scan. The fusion of multiple features will contain more information and thereby helping to improve FR performance. Third, we will investigate other weights assigned to descriptors according to their relevance.

References

[1] Phillips, P. Jonathon, Flynn, Patrick J., Scruggs, Todd, et al. Overview of the face recognition grand challenge. In : Computer vision and pattern recognition, 2005. CVPR 2005. IEEE computer society conference on. IEEE, 2005. p. 947-954.

[2] Li, Billy YL, et al. "Using kinect for face recognition under varying poses, expressions, illumination and disguise." Applications of Computer Vision (WACV), 2013 IEEE Workshop on. IEEE, 2013.

[3] Pamplona Segundo, Mauricio, Sarkar, Sudeep, Goldgoe, Dmitry, et al. Continuous 3D face authentication using RGB-D cameras. In : Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition Workshops. 2013. p. 64-69.

[4] Ciaccio, Cesare, Lingyun Wen, and Guodong Guo. "Face recognition robust to head pose changes based on the RGB-D sensor." Biometrics: Theory, Applications and Systems (BTAS), 2013 IEEE Sixth International Conference on. IEEE, 2013.

[5] Goswami, Gaurav, Bharadwaj, Samarth, VATSA, Mayank, et al. On RGB-D face recognition using Kinect. In : Biometrics: Theory, Applications and Systems (BTAS), 2013 IEEE Sixth International Conference on. IEEE, 2013. p. 1-6.

[6] Goswami, Gaurav, Mayank Vatsa, and Richa Singh. "RGB-D Face Recognition With Texture and Attribute Features." IEEE Trans. Information Forensics and Security 9.10 (2014): 1629-1640.

[7] Cardia Neto, Joo Baptista et MARANA, Aparecido Nilceu. 3DLBP and HAOG fusion for face recognition utilizing Kinect as a 3D scanner. In: Proceedings of the 30th Annual ACM Symposium on Applied Computing. ACM, 2015. p. 66-73.

[8] Boutellaa, Elhocine. Contribution to Face Analysis from RGB Images and Depth Maps. Diss. Ecole nationale Suprieure en Informatique Alger, 2017.

[9] Azzakhnini, Safaa, Lahoucine Ballihi, and Driss Aboutajdine. "Combining Facial Parts For Learning Gender, Ethnicity, and Emotional State Based on RGB-D Information." ACM Transactions on Multimedia Computing, Communications, and Applications (TOMM) 14.1s (2018): 19.

[10] Dreuw, Philippe, et al. "SURF-Face: Face Recognition Under Viewpoint Consistency Constraints." BMVC. 2009.

[11] Du, Geng, Fei Su, and Anni Cai. "Face recognition using SURF features." MIPPR 2009: Pattern Recognition and Computer Vision. Vol. 7496. International Society for Optics and Photonics, 2009.

[12] Yunqi, Lei, Lai Haibin, and Jiang Xutuan. "3D face recognition by SURF operator based on depth image." Computer Science and Information Technology (ICCSIT), 2010 3rd IEEE International Conference on. Vol. 9. IEEE, 2010.

[13] Ajmera, Rahul, Aditya Nigam, and Phalguni Gupta. "3D face recognition using kinect." Proceedings of the 2014 Indian Conference on Computer Vision Graphics and Image Processing. ACM, 2014.

[14] Bentaieb, Samia, et al. "Face recognition from unconstrained three-dimensional face images using multitask sparse representation." Journal of Electronic Imaging 27.1 (2018): 013008.

[15] Colombo, Alessandro, Claudio Cusano, and Raimondo Schettini. "3D face detection using curvature analysis." Pattern recognition 39.3 (2006): 444-455.

[16] Szeptycki, Przemyslaw, Mohsen Ardabilian, and Liming Chen. "A coarse-to-fine curvature analysis-based rotation invariant 3D face landmarking." Biometrics: Theory, Applications, and Systems, 2009. BTAS'09. IEEE 3rd International Conference on. IEEE, 2009.

[17] Mahoor, Mohammad H., and Mohamed Abdel-Mottaleb. "3D face recognition based on 3D ridge lines in range data." Image Processing, 2007. ICIP 2007. IEEE International Conference on. Vol. 1. IEEE, 2007.

[18] Tang, Yinhang, et al. "3D face recognition with asymptotic cones based principal curvatures." Biometrics (ICB), 2015 International Conference on. IEEE, 2015.

[19] Tang, Yinhang, et al. "Principal curvature measures estimation and application to 3D face recognition." Journal of Mathematical Imaging and Vision 59.2 (2017): 211-233.

[20] Berretti, Stefano, et al. "Matching 3D face scans using interest points and local histogram descriptors." Computers and Graphics 37.5 (2013): 509-525.

[21] Koenderink, Jan J., and Andrea J. Van Doorn. "Surface shape and curvature scales." Image and vision computing 10.8 (1992): 557-564.

[22] Bay, Herbert, et al. "Speeded-up robust features (SURF)." Computer vision and image understanding 110.3 (2008): 346-359.

A novel image encryption approach using polar decomposition and orthogonal matrices

Oussama Noui
Department of Physics, Faculty of Sciences of Matter

University of Batna1, Algeria
oussama.noui@univ-batna.dz

Amine Barkat
Department of Electronics, Information, and Bioengineering,

Politecnico di Milano, Italy
amine.barkat@polimi.it

Assia Beloucif
Institute of Hygiene and Industrial Safety

University of Batna2, Algeria
a.beloucif@univ-batna2.dz

***Abstract*— Information security is one of the important issues in the information age, image encryption algorithms have been increasingly studied to guarantee the secure im-age transmission over the internet and through wireless networks. In this article, we propose a new approach for image encryption based on polar decomposition and orthogonal matrices. This scheme offers good confusion and diffusion qualities.**

The proposed algorithm is shown to be secure against important cryptanalytic attacks (statistical attacks, sensitivity dependence, differential attacks, brute force attacks...), theoretical analysis and computer simulations both confirm that it has a high security level.

Keywords—: encryption, security, digital image, orthogonal matrix, polar decomposition, information

I. INTRODUCTION

In recent years digital image processing technology and network technologies have been developed rapidly, a vast number of digital images are now transmitted and shared over the Internet; Confidentiality of such content became an important issue nowadays.

Furthermore the conventional encryption methods such as RSA AES, IDEA, DES, 3DES etc.[1]., are computationally intensive because they consume more time and are not suitable for images, this is due to the digital image properties like high redun-dancy, bulk volume and high correlation among adjacent pixels.

To meet this challenge, a variety of encryption schemes have been proposed, [2-10], recently there has been a growing interest in chaotic based image encryption , because they offer good properties in many concerned aspects regarding speed, secu-rity, computing power, complexity and computational overhead.

The security of the cryptosystems based on chaotic stands on the used chaotic map and the adopted architecture, some chaotic based methods have security problems which are related to the small size of secret key and to the used chaotic map properties [11-14].

In this paper we concentrates on developing of highly robust encryption scheme which offer good confusion by using the polar decomposition and the orthogonal matrices and offers good diffusion qualities based on the polynomial permutation matrix, and to ensure popular security factor, and to prevent statistical, differential and exhaustive attacks, and to be economically in term of time complexity.

Organization of the rest of this paper is as follows: Section II explains the related knowledge, including the polar decomposition, the singular values decomposition and the polynomial permutation, section III presents the encryption and decryption algorithms and the key generation procedure, in section IV we study the performance and the security analysis, including statistical analysis and sensibility analysis, whereas the summary of results and the conclusion is presented in Section V.

II. 2 RELATED KNOWLEDGE

A. *Polar decomposition*

Let be a matrix with real entries, the left polar decomposition of is with is orthogonal and is symmetric matrix with non negative eigenvalues.

B. *Singular values decomposition (SVD)*

A notion is closely related to the polar decomposition is the singular values decomposition:

Theorem [15]

For any real $n \times n$ matrix A of rank r, we have

$$A = U\ S\ V^t \qquad (1)$$

Where U and V are two orthogonal matrices and S is a $n \times n$ diagonal matrix

$S = (\partial_1, .., \partial_r, 0.., 0)$ such that $\partial_1 \geq .. \geq \partial_r \geq 0$ are the singular values of A.

C. *Computation of the polar form from SVD*

It is easy to go from the SVD to the polar form:

$$A = U\ S\ V^t = (U\ S\ U^t)\ (U\ V^t) \qquad (2)$$

Put $P = U\ S\ U^t$ (P is symmetric matrix with non negative eigenvalues).

And $Q = U\ V^t$ (Q is a product of two orthogonal matrices then Q is so)

Hence $A = P\ Q$ is the polar form of A.

D. *Permutation polynomial modulo* 2^n

A polynomial $f(x)$ with integral coefficients is said to be a permutation polynomial over a finite ring R if f is one to one map of R onto itself.

In [16] Rivest proved that A polynomial $f(x) = a_0 + a_1 x + ... + a_d x^d \in Z[x]$ is a permutation polynomial modulo 2^n, $n > 1$, if and only if a_1 is odd, $(a_2 + a_4 + ...\ )$ and $(a_3 + a_5 + ...\ )$ are even.

III. PROPOSED METHOD

Let $A = (a_{ij})$ be a gray scale image of size n, (we take n = 256 for tests), the proposed encryption scheme follows these steps:

A. Image encryption

Let A be an image of size 256.

Input: three keys: K_1, K_2, K_3 to generate respectively three matrices:

U_1 is 256×256 orthogonal matrix with real entries.

U_2 is permutation matrix of order 256.

$D=(\pm 1)$ is a diagonal matrix of size 256.

Output: A^* : The encrypted image.

1. Apply SVD and polar decomposition to $A=U\,S\,V^t=P\,Q$
2. Compute $P^*=P^{U_1}=U_1\,P\,U_1^t$
3. Calculate $Q^*=D\,U_1\,Q\,U_1\,U_2$
4. Calculate the cipher image $A^*=P^*Q^*$

B. Image decryption

Input: A^* the encrypted image, the three keys K_1, K_2, K_3.

1. Apply polar decomposition to $A^*=P^*Q^*$
2. Calculate $P=P^{*U_1^t}=U_1^tP^*U_1$
3. Calculate $Q=U_1^t\;D\,Q^*\;U_2^t\,U_1^t$
4. Finally compute the original image $A=P\,Q$

C. Generation of U_1

Using the method in [17], to generate an 256×256 orthogonal matrix U_1 from a random sequence $K_1^{'}=(x_1,..,x_{255})$ we put

$$A_0=\begin{pmatrix} 0 & -x_1 & \cdots & -x_{255} \\ x_1 & 0 & \cdots & 0 \\ \vdots & \vdots & & \vdots \\ x_{255} & 0 & \cdots & 0 \end{pmatrix}$$

and $\partial=\sqrt{x_1^2+..+x_{255}^2}$,

Then

$$U_1=I_{256}+\frac{\sin\partial}{\partial}A_0+\frac{1-\cos\partial}{\partial^2}A_0^2$$

is orthogonal

To obtain a good sensitive dependence we generate the sequence K_1 from a logistic map $x_{n+1}=\mu\,x_n(1-x_n)$ with the initial value $x_0\in\,]\,0,1\,]$

And $\mu\in[3.57,4]$ so the first key $K_1=\{\,x_0,\,\mu\,\}$ is needed to generate the orthogonal matrix U_1.

D. Generation of permutation matrix U_2

In order to construct, U_2 we use the permutation polynomial modulo $2^8=256$

Indeed, we choose an integer a_0 and an even integer a_2 from $\{1,..,256\}$ then, by (*), the polynomial $P(x)=a_0+x+a_2x^2$ define a permutation in the set $\{1,..,256\}$.

Let U_2 the permutation matrix associated to $P(x)$. Hence for the generation

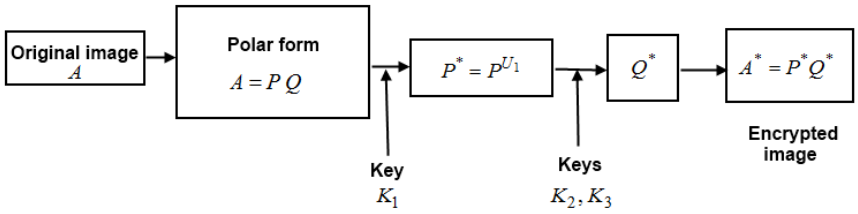


Figure 1. Block diagram of the encryption procedure.

of U_2 we need the key $K_2 = \{ a_0, a_2 \}$.

For generation of D we choose randomly a binary sequence K_3 of length 256, we replace the 0 by -1, the obtained sequence forms the diagonal of D. Figure 1 illustrates the block diagram of the proposed algorithm.

IV. Performance and Security Analysis

To study the feasibility of our image encryption scheme, we analyze its security against common cryptanalysis attacks.

A. Key space analysis

Generally, the security of an encryption algorithm mainly stands on its security key design [18]. The proposed method has a sufficiently large key space and high key sensitivity. The secret key in the proposed algorithm consists of three parts: K_1, K_2, K_3.

For the first key, $K_1 = \{ x_0, \mu \}$ according to the IEEE floating point standard, the number of possible values of K_1 is about $10^{15} \times 10^{15}$.

For the second key $K_2 = \{ a_0, a_2 \}$, $a_0, a_2 \in \{1, .., 256\}$ as a_2 is even, we have 256×128 combinations. As the key K_3 is a random binary sequence of length 256 we have 2^{256} combinations to obtain the third key, thus size of key space of our scheme is greater than $10^{30} \times 256 \times 128 \times 2^{256} > 2^{360}$, hence the key space is large enough to resist brute force attack.

B. Cipher image only attack

The illegal user needs to obtain the keys K_1, K_2, K_3 from the cipher image

$$A^* = (U_1 P U_1^t)(D U_1) Q (U_1 U_2) \quad (3)$$

If we encrypt A, on m rounds, we obtain the cipher image

$$A^{(m)} = U_1^m P (U_1^t)^m (D U_1)^m Q (U_1 U_2)^m \quad (4)$$

Hence the calculation of U_1, U_2 and D from (3) or (4) becomes ineffective.

C. Statistical analysis

According to Shannon's theory, a secure cryptographic scheme should be strong enough to resist statistical attack.
For the statistical analysis, our image encryption scheme is tested using most known statistical measures which includes histogram, information entropy

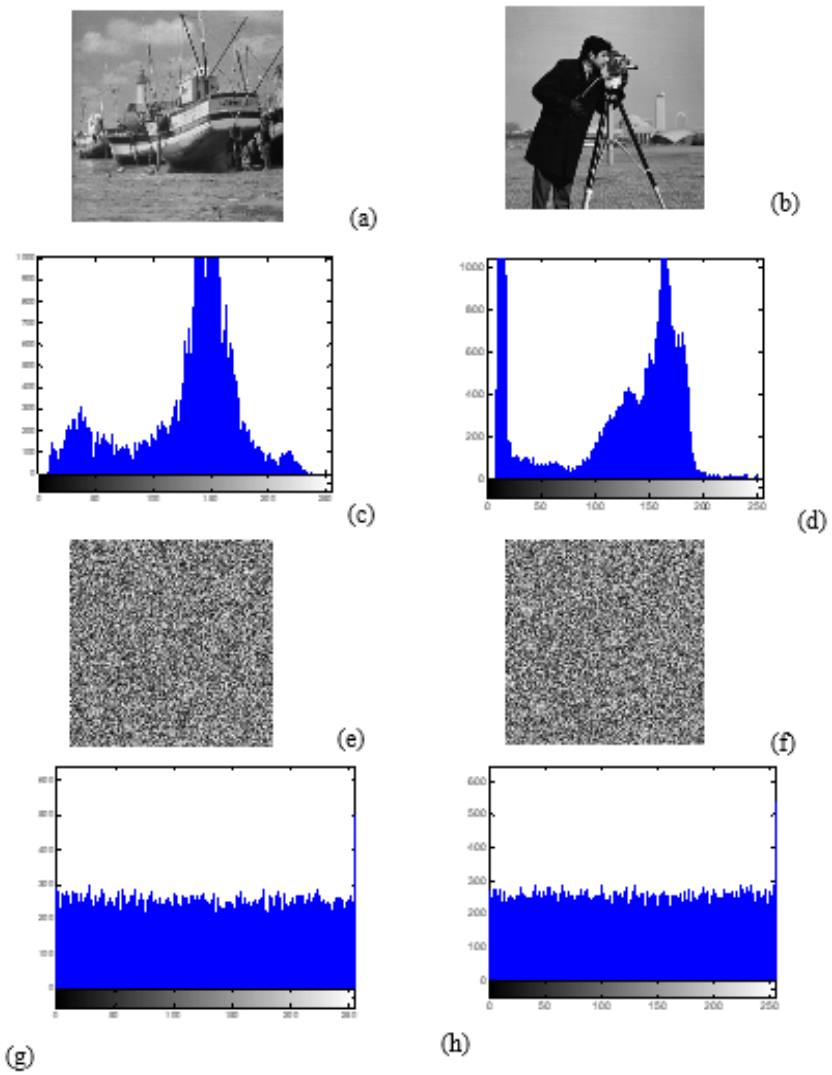


Figure 2. Statistical analysis

Table 1. Entropy results for the cipher images

Encrypted image	Cameraman	Boat	Baboon	Lena	Peppers
Entropy	7.9325	7.9520	7.9461	7.9801	7.9932

and adjacent correlation analysis, in the first experiment we encrypted two images of size 256, figure (2) as (a,b), as its seen in figure 2, the histogram charts of both encrypted test images (g,h) are uniform which represents the distribu-

tion intensity of pixels values in the encrypted image, this results makes statistical attacks difficult.
The uniformity is justified by chi-square test, which is described by the following expression:

$$x^2 = \sum_{k=1}^{256} \frac{(V_k - 256)^2}{256} \qquad (5)$$

Where k is the number of gray levels (256), V_k is the observed occurrence frequencies of each gray level (0–255). The lower value of the chi-square value indicates a better uniformity.
The second statistical measure is the entropy which is one of the best functions for calculating and measuring the randomness of image encryptions algorithms.
The information entropy *H(m)* of a message source *m* can be computed as:

$$H(m) = \sum_{i=0}^{2^n-1} p(m_i) \log_2 \frac{1}{p(m_i)} \qquad (6)$$

Ideally, the information entropy should be 8 bits for grayscale images. If an encryption scheme generates an output cipher image whose entropy is less than 8 bits, then there would be a possibility of predictability, which may threaten its security.
Simulation results for entropy analysis are shown in Table1. It is clear from table 1, that the values of entropy of the encrypted test images are very close to

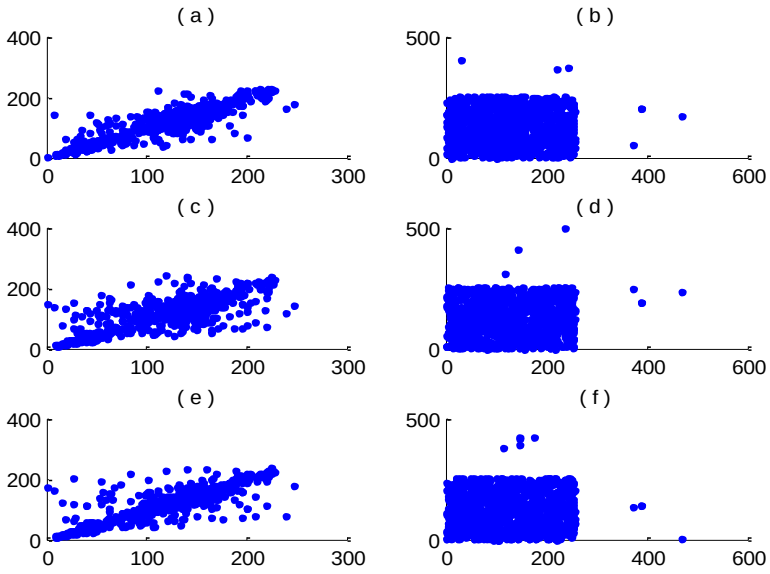


Figure 3 Correlation of two adjacent pixels

(a) Distribution of two horizontally adjacent pixels in the plain image (b) Distribution of two horizontally adjacent pixels in the cipher-image, (c) Distribution of two diagonally adjacent pixels in the plain-image (d) Distribution of two diagonally adjacent pixels in the cipher-image (e) Distribution of two vertically adjacent pixels in the plain-image (f) Distribution of two vertically adjacent pixels in the cipher-image

theoretical value of 8 bits. This implies that our encryption algorithm is secure against entropy attack, while the third measure is the correlation analysis, Correlation determines the connection between two variables. In other terms, correlation is a measure that determines level of similarity between two variables. Correlation coefficient is a useful evaluation to judge encryption quality of any cryptosystem.

Generally for any plain image, each pixel is highly correlated with its adjacent pixels in all the three directions: horizontal, vertical and diagonal. A good encryption will erase this correlation between adjacent pixels.

The correlation coefficients were calculated using the following equations:

$$C = \frac{\frac{1}{N}\sum_{i=1}^{N}(x_i - \bar{x})(y_i - \bar{y})}{\sqrt{\left(\frac{1}{N}\sum_{i=1}^{N}(x_i - \bar{x})^2\right)\left(\frac{1}{N}\sum_{i=1}^{N}(y_i - \bar{y})^2\right)}} \quad (7)$$

with $\bar{x} = \frac{1}{N}\sum_{i=1}^{N} x_i$, $\bar{y} = \frac{1}{N}\sum_{i=1}^{N} y_i$

Where x and y are grey-level values of the two adjacent pixels in the image.

The correlation distributions of Cameraman test image are shown in Figure 3.

V. SENSIBILITY ANALYSIS

A. Chosen plaintext attack.

The attacker has obtained access to the encryption machinery, he makes a minor change of the plain text and examines the obtained cipher text.

As the values of NPCR and UACI are larger, the large changes in the cipher text do not give any useful information to the attacker.

NPCR and UACI: number of pixel change rate (NPCR) and unified average change intensity (UACI) are two common measures used to examine the impact of one pixel modify on the whole image, encrypted by an algorithm. NPCR measures the percentage of the number of different pixels to the total number of pixels. In brief NPCR, it means that the number of pixels change rate of ciphered image while one pixel of plaintext image is changed.

Let C_1 and C_2 be two different cipher-images whose corresponding plaintext images are differ by only one bit. Label the grayscale value of the pixel at grid (i, j) in C_1 and C_2 by $C_1(i, j)$ and $C_2(i, j)$ respectively. Define an array, D, the same size as images C_1 and C_2. Then $D(i, j)$ is determined by $C_1(i, j)$ and $C_2(i, j)$ namely, if $C_1(i, j) = C_2(i, j)$ then $D(i, j) = 0$, otherwise, $D(i, j) = 1$

The NPCR is defined as:

$$NPCR = \frac{\sum_{i,j} D(i, j)}{W \times H} \times 100\% \quad ((7)$$

Where W and H are the width and height of cipher images C_1 and C_2.

To examine the average intensity of differences between the images, UACI is used to check the impact of one pixel change, UACI is defined as:

$$UACI = \frac{1}{W \times H}\left[\sum_{i,j} \frac{C_1(i, j) - C_2(i, j)}{255}\right] \times 100\%$$

Table 2 shows the NPCR and UACI results of our method on a different test images, the obtained results prove that

Table 2 . NPCR and UACI of encrypted-images

Test images	Lena	Cameraman	Baboon	Boat	Peppers
NPCR	99.5230	99.6902	99.2131	99.6150	99.3874
UACI	31.2013	32.0626	33.1245	32.5132	31.8709

the proposed method can resist differential attack.

*B. **Remarks**.*

1. The key $K = K_1 \| K_2 \| K_3$ of the proposed scheme is flexible, we have the ability to increase the size of the key, for example for K_2 we take a polynomial of degree r , $P(x) = a_0 + a_1 x + ... + a_r x^r$ and $K_2 = \{ a_0, a_1, .., a_r \}$ such that a_1 is odd and $a_2 + a_4 + ...$ and $a_3 + a_5 + ...$ are even.

2. The key length and the number of rounds are chosen following the desired level of security.

VI. CONCLUSION

The security is an essential part of any communication system. This paper proposed an image encryption based on polar decomposition and orthogonal matrices.

Permutation matrix is used to achieve the diffusion property; the orthogonal matrix is used to realize the confusion property.

Theoretical analysis and experimental results show that the proposed scheme able to resist known attacks, the used algorithm has a flexible key, its length is chosen following the desired security level.

REFERENCES

1. SINGH, Gurpreet et SUPRIYA, A. A Study of Encryption Algorithms (RSA, DES, 3DES and AES) for Information Security. International Journal of Computer Applications, 2013, vol. 67, no 19, p. 33-38.
2. Chen, Guanrong, Yaobin Mao, and Charles K. Chui. "A symmetric image encryption scheme based on 3D chaotic cat maps." *Chaos, Solitons & Fractals*21.3 (2004): 749-761.
3. Wang, Bin, et al. "Evaluating the permutation and diffusion operations used in image encryption based on chaotic maps." Optik-International Journal for Light and Electron Optics (2016).
4. Tang, Zhenjun, et al. "Multiple-image encryption with bit-plane decomposition and chaotic maps." Optics and Lasers in Engineering 80 (2016): 1-11.
5. Yang, Huaqian, et al. "A fast image encryption and authentication scheme based on chaotic maps." Communications in Nonlinear Science and Numerical Simulation 15.11 (2010): 3507-3517.
6. Fu, Chong, et al. "A novel chaos-based bit-level permutation scheme for digital image encryption." Optics communications 284.23 (2011): 5415-5423.
7. Mannai, Olfa, et al. "A new image encryption scheme based on a simple first-order time-delay system with appropriate nonlinearity." Nonlinear Dynamics82.1-2 (2015): 107-117.
8. Chen, Jun-xin, et al. "A fast chaos-based image encryption scheme with a dynamic state variables selection mechanism." Communications in Nonlinear Science and Numerical Simulation 20.3 (2015): 846-860.
9. Zhao, Jianfeng, et al. "A novel image encryption scheme based on an improper fractional-

order chaotic system." Nonlinear Dynamics 80.4 (2015): 1721-1729.
10. Kanso, A., and M. Ghebleh. "An efficient and robust image encryption scheme for medical applications." Communications in Nonlinear Science and Numerical Simulation 24.1 (2015): 98-116.
11. Bechikh, Rabei, et al. "Breaking an image encryption scheme based on a spatiotemporal chaotic system." Signal Processing: Image Communication 39 (2015): 151-158.
12. Akhavan, A., A. Samsudin, and A. Akhshani. "Cryptanalysis of “an improvement over an image encryption method based on total shuffling”."Optics Communications 350 (2015): 77-82.
13. Rhouma, Rhouma, and Safya Belghith. "Cryptanalysis of a new image encryption algorithm based on hyper-chaos." Physics Letters A 372.38 (2008): 5973-5978.
14. Li, Shujun, and Xuan Zheng. "Cryptanalysis of a chaotic image encryption method." Circuits and Systems, 2002. ISCAS 2002. IEEE International Symposium on. Vol. 2. IEEE, 2002.
15. G. H. GOLUB AND C. F. VAN LOAN, Matrix Computations, Johns Hopkins University Press, Baltimore,MD, 1983.
16. R.L.Rivest, permutation polynomials modulo 2^n , finite fields and their applications, 7, 287- 292, 2001.
17. Oussama, Noui, Beloucif Assia, and Noui Lemnouar. "Secure image encryption scheme based on polar decomposition and chaotic map." International Journal of Information and Communication Technology 10.4 (2017): 437-453.
18. Beloucif, Assia, Oussama Noui, and Lemnouar Noui. "Design of a tweakable image encryption algorithm using chaos-based schema." International Journal of Information and Computer Security 8.3 (2016): 205-220.

Community structure in complex networks based on Tabu Search

1st Bilal SAOUD
Department of Electrical Engineering
Bouira University
Bouira, Algeria
bilal340@gmail.com

***Abstract*—Many problems have been solved by heuristic methods. Among these heuristics we find Tabu Search. In our paper, we propose a new community detection method in complex networks based on Tabu Search. In this method we use a Tabu Search to split networks and find the community structure that maximizes the function of quality called modularity. We repeat splitting process several times. At the end each node represents a community. The community structure, that has the highest value of modularity will be selected. We provide a general framework for implementing our method. Simulation results of comparison of our method and others on computer-generated and real world networks reflect the effectiveness of our method.**

***Index Terms*—community detection, networks, Tabu Search, normalized mutual information, modularity**

I. Introduction

Network or graph can represent many complex systems shush as biology, computer science, linguistics, etc. A network (graph) has a two sets, the first one is vertex (or node) set and the second is edge set. Vertexes represent system individuals members and edges represent the relationship between nodes. For example, in a computer network, a computer is represented by a node, and the connection of two connected computers is represented by an edge. Using networks can help to understand complex systems. For this reason to understand a complex system we need to understand its represented network. The most important feature in a network is the existence of parts (nodes and edges) more densely connected than other parts. Each part, which is set of nodes and edges, is called a community. Finding communities in network allows us to understand the structure and relationship between nodes. Finally, the different communities in network is called a community structure.

Recently, the community structure detection in networks has become very active domain of research. It is an NP-hard problem [1]. In generally, there is no information about the number of communities that should be found and the size of communities. Many methods have been proposed to find community structure in network, however the problem is not yet satisfactorily resolved. Some methods find community structure for directed or undirected networks, weighted or unweighted networks. Furthermore, methods can be classified according to the type of networks (unipartite or bipartite, weighted or unweighted, directed of undirected) and community structure can be disjoint or overlapping [1], [2]. In our study we focused on methods for uniparitie, unweighted networks in order to find disjoint community structure.

Our method can find community structure in unweighted and undirected networks. We have used a Tabu Search heuristic to optimize the function of quality called modularity. Our method takes a graph $G(V, E)$ like an input and find the most optimal community structure $\pi = \{c_1, ..., c_k\}$. Where $\bigcup_{i=1}^{k} c_i = V$ and $c_i \neq \emptyset$, $c_i \cap c_j = \emptyset$ (for $i, j = 1 : k$). At first Tabu Search Algorithm has been used to split the network G into new graphs G_1 and G_2. The graph G_1 represents a community c_1 and the graph G_2 represents a community c_2. The splitting is based on the Tabu Search in order to maximize the value of modularity function Q. Each of graphs G_1 and G_2 will be split until the graph G has been disconnected (each node of G represents a community). We choose the community structure that gives a high value of Q. The paper is organized as follow. The concept of Tabu Search algorithm is presented in section II. Our approach is detailed in section III. Experimental results are shown in section IV. Finally, we conclude our paper in section V.

II. Tabu Search

The Tabu Search (TS) is a metaheuristic search algorithm that was created in 1986 by Fred Glover [3]. This metaheuristic employs local search methods used for mathematical optimization. TS can be used to solve many combinatorial optimization problems in different fields.

The idea of the TS method is to iteratively explore the search space of all feasible solutions by a sequence of moves. At each iteration moves from one potential solution x to an improved solution x', and the process stops when some criterion has been satisfied. To avoid some problems like local minima [4] a selection of moves has been added to the ST method.

The TS requires some elements to be defined. Among these elements we find:

- Solution representation: Each feasible solution to the optimization problem must have a unique representation

within the search space. In our case, the space of search is represented by integers from 1 to $n = |V|$.

- Cost function: A function cost mapping each feasible solution into a value representing its optimization cost. The goal of the algorithm is to find a solution that optimizes this value. In our case, the cost function is the modularity [4].
- Neighbourhood: A function mapping each feasible solution into a set of other solutions. Each time the algorithm has to consider a new solution, it is chosen from the neighbourhood of the current solution.
- Tabu list: It is an important tool in guiding the search in the short term, given the determination of an effective set of attributes for defining tabu status. It contains the last moves carried out, which, for this reason, are forbidden. A solution obtained from the current solution S with a move contained in the tabu list cannot be a member of the neighbourhood of S.
- Aspiration criterion: The level for which aspiration overrides tabu status is a sensitive key factor in the search as this defines the degree of flexibility of the method. One common-sense-based approach is to relax the tabu restriction if a solution happens to produce a better result than the currently best-known solution and it can be considered to be in the neighbourhood of S.
- Termination Criteria: One may have noticed that we have not specified in our template a termination criterion. In theory, the search could go on forever, unless the optimal value of the problem at hand is known beforehand. In practice, obviously, the search has to be stopped at some point. In generally, there are some criteria that can be used:
  - After a fixed number of iterations;
  - After some number of consecutive iterations without an improvement in the objective function value;
  - When the objective function reaches a pre-specified threshold value.

III. Our method to discover community structure in complex networks

In this section we are going to describe our method to find the community structure in networks. We proposed an approach for networks (graphs) which are unipartite, undirected and unweighted. Our method does not need the number of communities that should be found. For a graph $G(V, E)$ our method will find the most optimal community structure $\pi = \{c_1, ..., c_k\}$. Where $\bigcup_{i=1}^{k} c_i = V$ and $c_i \neq \emptyset$, $c_i \cap c_j = \emptyset$ (for $i, j = 1 : k$).

Many hierarchical methods have been proposed (divisive and agglomerative methods) over years. Our method is divisive algorithm. Some divisive methods are based on removing the edges between vertex pairs with lowest similarity, but in our method we divide the entire network into two networks based on the maximization of the modularity [4], [13]. To find the partition with two groups of a network, which maximizes the modularity, we based on the Tabu Search algorithm.

Modularity [4], [12] is one way to measure the strength of a community. Modularity Q is based on the observed fraction $e(c_i)$ of edges within communities and the expected fraction $a(c_i)$ of edges within the same communities, $Q = \sum_{c_i} e(c_i) - a(c_i)^2$. For an undirected and unweighted graph G, with n vertices and m edges, whose vertices are grouped in communities $(c_1, ..., c_k)$. Let i be a vertex, d_i its degree, and c_i its community. $A_{n,n}$ is the adjacency matrix of the graph, and $P_{n,n}$ is the adjacency matrix of the corresponding null model, where $P_{n,n} = \frac{d_i \times d_j}{2m}$ is the probability in the null model such that there is an edge between vertices i and j. The detailed expression of the modularity is given as follow:

$$Q = \frac{1}{2m} \sum_{i} \sum_{j} (A[i, j] - P[i, j]) \delta(c_i, c_j) \qquad (1)$$

where

$$\delta(c_i, c_j) = \begin{cases} 1 \; if \; c_i = c_j \\ 0 \; otherwise \end{cases}$$

Q closer to 1 indicates stronger community structures.

Let an undirected and unweighted network $G(V, E)$, where $V = (v_1, v_2, ..., v_n)$ is the set of vertices, $E = (e_1, e_2, ..., e_m)$ is the set of edges. The goal of our community detection method is to partition the network G into k communities (groups): $\pi = \{c_1, c_2, ..., c_k\}$, where $c_i \neq \emptyset$, $c_i \cap c_j = \emptyset$, $(i = 1 : k, j = 1 : k)$ and $V = \bigcup_{i=1}^{k} c_i$. And the value of the modularity Q of the graph G with the community structure π is the greatest. To reach this goal we used a Tabu Search (TS) algorithm to find a community structure with two communities (to divide the network into two networks) which gives us a good value of modularity Q. The cost function of the TS algorithm is the modularity function (equation 1). And we repeat these steps of dividing the networks until we separate all the nodes of the two new networks (each community has one node).

Thus the general form of our community structure finding algorithm is as follows:

Data: $G(V, E)$
Result: dendrogram
$\pi = TB()$, find a partition π based on Tabu Search algorithm;
Divide G based π, $G = G_1 + G_2$;
Update the matrix of merge M for a final dendrogram;
Go to *Steps 1* for each graph G_1 and G_2;
Return the final dendrogram;
Algorithm 1: The algorithm of the proposed method

After we got the dendrogram, we can choose a community structure based on the number of communities or the value of modularity. Fig 1 shows the dendrogram that was found by our method for Zachary's Karate Club [6].

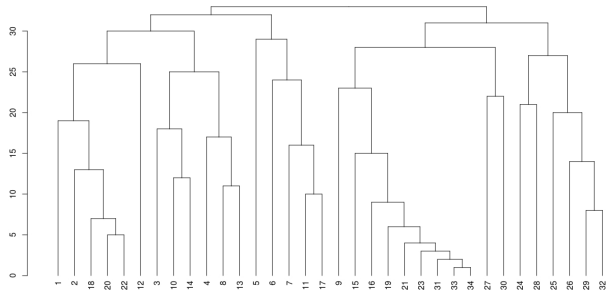


Fig. 1. The dendrogram of Zachary's Karate Club network created by our method

IV. Experiment and results

In this section, we evaluate the effectiveness and efficiency of our method. Our experiment is to demonstrate the performance of our approach to find disjoint communities on computer-generated and several real networks (Zackary's Karate Club, American College Football, Dolphins and Books about US Politics). The results of our approach are compared with results obtained by well-known methods: Walktrap method [11], Fast Greedy method [5], Louvain method [7] and Label Propagation method [8].

A. Performance measure

To compare our approach to other existing works, we used the metric of normalized mutual information [9]. This metric allows us to compare the community structure that was founded by methods with the real community structure. It is based on defining a confusion matrix N, where the rows correspond to the real communities, and the columns correspond to the found communities. The element of N, N_{ij} is the number of nodes in the real community that appear in the found community j. The formula based on information theory of similarity between two partitions A and B, is:

$$I(A,B) = \frac{-2\sum_{i=1}^{c_A}\sum_{j=1}^{c_B} N_{ij}\log(\frac{NijN}{N_{i.}N.j})}{\sum_{i=1}^{c_A} N_{i.}\log(\frac{N_i}{N}) + \sum_{j=1}^{c_B} N_{.j}\log(\frac{N_{.j}}{N})} \quad (2)$$

c_A represents the number of real communities, c_B represents the number of found communities.

B. Computer-generated networks

The proposed method is tested on computer-generated networks benchmark proposed by Lancichinetti et al. [10]. The benchmark parameters are the number of nodes N; the exponents γ and β of the degree and community size distribution respectively (both distributions are power laws); the number of average degree $\langle k\rangle$; number of communities N_c; and the mixing parameter μ. Each node shares a fraction $1-\mu$ of its links with other nodes of its community and a fraction μ with the other nodes of the network.

Fig. 2 shows the variation of the normalized mutual information obtained by the proposed method and Walktrap method, Fast greedy method, Label propagation method and Louvain method on the benchmarks networks, with

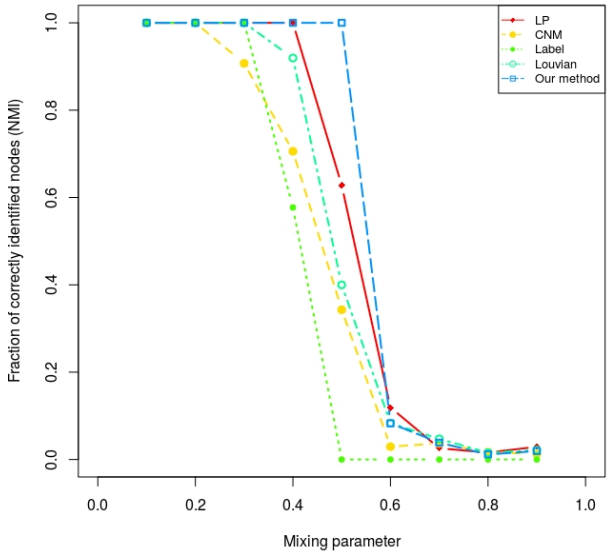


Fig. 2. NMI vs. mixing parameter μ

the parameters: mixing parameter μ between 0.1 and 0.9, $\langle k\rangle = 16$, $\gamma = 3$, $\beta = 2$, $N = 128$ and $N_c = 4$.
The value of NMI obtained by our approach is 1 when μ changes from 0 to 0.5, which means that the proposed algorithm can find the true community structure correctly. When μ equals 0.6, it is difficult for all the methods to find the true community structure, but our method is still more accurate than the other methods. From Fig 2 we see that our approach could discover community structure more better than Walktrap, Fast greedy, Louvain and Label propagation method.

Fig. 3 shows the values of modularity of each methods on the different networks which were generated by computer. Our method gives a good value of modularity. According to Clauset et al. [5] a value above about 0.3 is a good indicator of significant community structure in a network.

C. Real networks

In this section, we give the simulation results of our approach, Walktrap, Fast greedy, Louvain and Label propagation on real networks. We considered some real networks drawn from disparate fields (Zachary, Dolphins, Football and Books), where the community structure is known, which made them suitable to evaluate community detection methods.

1) Zachary's club network [6] is a real network that corresponds to a social network of friendships between 34 members of a karate club at a university in the United States in the 1970 ($n = 34$ and $m = 78$). The network has two clusters.
2) Dolphins Network [14] is an undirected social network of frequent associations between 62 dolphins in a community living off Doubtful Sound, New Zealand. This networks ($n = 62$ and $m = 159$) has two communities.
3) College football network [15] represents the schedule of Division I Games for the year 2000 season. This network

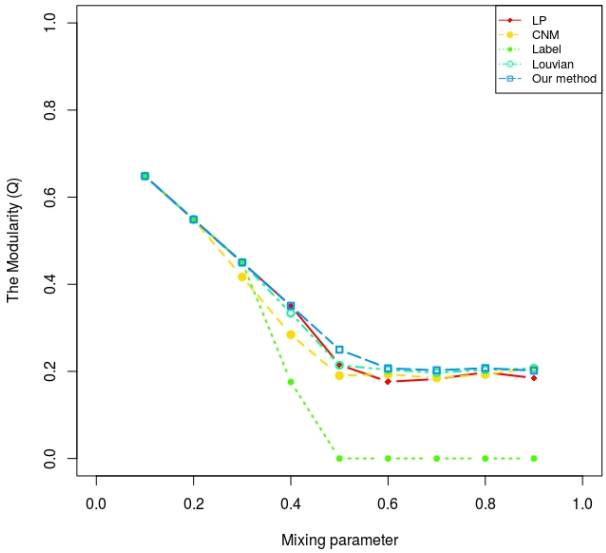


Fig. 3. Modularity values vs. mixing parameter μ

is made of 115 teams (nodes) and 613 edges. It is divided into 12 groups.

4) Books about US politics Network [16] is a network of books about US politics published around the time of the 2004 presidential election and sold by the online bookseller Amazon.com. Edges between books represent frequent purchasing of books by the same buyers. Compiled by Valdis Krebs. Books network has three communities.

Table I gives obtained results on networks. As can be seen from Tables 1, our method can regroup the most nodes in the correct communities on Zachary's karate club, the dolphin social network, American college football and books about US politics. Fig 4 and 5 show the community structure that was found by our method on Zachary's karate club and football network.

V. Conclusion and Future Work

Many community detection methods have been proposed. Some methods are based on similarity between nodes others on maximization of modularity but we find few methods witch are based on heuristics. In this work we have presented our new method to find disjoint communities in complex networks. The method is based on Tabu Search algorithm to split a network (graph) into two networks and this process of splitting is repeated until all the edges are removed. The method is constructed for undirected and unweighted networks. Our method is designed for undirected and unweighted networks. Results obtained on computer-generated networks and real world networks proved the efficiency of our method.
We can extend our method in order to detect overlapping between communities. The method can be improved to find the community structure in directed/weighted networks.

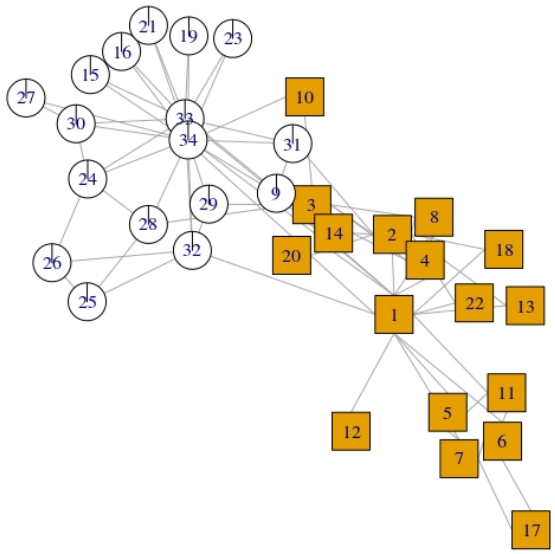


Fig. 4. Zachary's karate club network structure is detected by the proposed method and represented by different colors and shapes

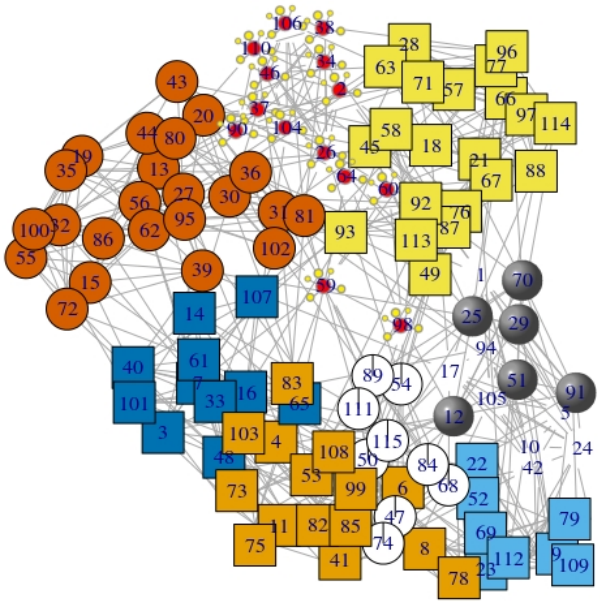


Fig. 5. The football network structure is detected by the proposed method and represented by different colors and shapes

References

[1] S. Fortunato, "Community detection in graphs", Phys Rep. 486, 75-174, 2010.
[2] S. Fortunato and D. Hric,"Community detection in networks: A user guide," Physics Reports, 659, 1-44, 2016.
[3] F. Glover, "Future Paths for Integer Programming and Links to Artificial Intelligence," Computers and operations research. 13 (5), 533-549, 1986.
[4] K.S. Al-Sultan, "A Tabu Search approach to the clustering Problem," Pattern Recognition. 28(9), 1443-1451, 1995.
[5] A. Clauset, M. E. Newman and C. Moore, "Finding community structure in very large networks," Physical review E, 70(6), 066111, 2004.
[6] W. W. Zachary, "An information flow model for conflict and fission

TABLE I
PERFORMANCE RESULTS ON REAL NETWORKS

Methods	Karate			Dolphins			Football			Books		
	$\|c\|$	NMI	Q	$\|c\|$	NMI	Q	$\|c\|$	NMI	Q	$\|c\|$	NMI	Q
$Walktrap$	4	0.69	0.41	4	0.58	0.48	10	0.87	0.60	4	0.54	0.50
$Fast\ greedy$	3	0.69	0.38	4	0.55	0.49	6	0.70	0.54	4	0.53	0.50
$Louvain$	4	0.58	0.41	5	0.46	0.51	10	0.87	0.60	5	0.50	0.52
$Label\ propagation$	2	1	0.37	3	0.86	0.37	9	0.85	0.59	4	0.56	0.51
$Our\ method$	2	0.83	0.37	3	0.60	0.51	10	0.82	0.56	2	0.59	0.45

in small groups," Journal of anthropological research, 33(4), 452-473, 1977.

[7] V. D. Blondel, J. L. Guillaume, R. Lambiotte and E.Lefebvre, "Fast unfolding of communities in large networks," Journal of statistical mechanics: theory and experiment, 2008(10), P10008, 2008.

[8] U. N. Raghavan, R. Albert and S. Kumara, "Near linear time algorithm to detect community structures in large-scale networks," Physical review E, 76(3), 036106, 2007.

[9] L. Danon, A. Diaz-Guilera, J. Duch and A. Arenas, "Comparing community structure identification," Journal of Statistical Mechanics: Theory and Experiment, 2005(09), P09008, 2005.

[10] A. Lancichinetti, S. Fortunato and F. Radicchi, "Benchmark graphs for testing community detection algorithms," Physical review E, 78(4), 046110, 2008.

[11] P. Pons and M. Latapy, "Computing communities in large networks using random walks," In International symposium on computer and information sciences, pp. 284-293. Springer, Berlin, Heidelberg, 2005.

[12] R. Shang, S. Luo, Y. Li, L. Jiao and R. Stolkin, "Large-scale community detection based on node membership grade and sub-communities integration," Physica A: Statistical Mechanics and its Applications, 428, 279-294, 2015.

[13] R. Shang, J. Bai, L. Jiao and C. Jin, "Community detection based on modularity and an improved genetic algorithm," Physica A: Statistical Mechanics and its Applications, 392(5), 1215-1231, 2013.

[14] D. Lusseau, K. Schneider, O. J. Boisseau, P. Haase, E. Slooten and S. M. Dawson, "The bottlenose dolphin community of Doubtful Sound features a large proportion of long-lasting associations," Behavioral Ecology and Sociobiology, 54(4), 396-405, 2003.

[15] M. Girvan and M. E. Newman, "Community structure in social and biological networks," Proc. Natl. Acad. Sci. USA, 99(cond-mat/0112110), 8271-8276, 2001.

[16] MEJ. Newman: Mark Newmans Network Data Collection, http://www-personal.umich.edu/ mejn/netdata/ (2019)

SIMULATION OF ATTACKS ON AUTHENTICATION PROTOCOLS FOR NEAR FIELD COMMUNICATIONS

Noureddine Chikouche

Computer Science Department
Mohamed Boudiaf University of M'sila
Algeria

ABSTRACT

Near Field Communication (NFC) technology is steadily becoming paramount due to its vast applications in domain of mobile services such as, payment, marketing, etc. The communication between the NFC tag and the NFC device is based on radio frequency which is unsecured. Several authentication protocols have been proposed to achieve the security requirements and to avoid different existing attacks (e.g. spoofing, denial of service, etc.). Recently, Beak and Youm proposed two versions of authentication protocol for NFC tag based services. Firstly, an NFC tag authentication protocol and the second is a NFC-enabled device authentication protocol. In this paper, we analyse the security of these protocols using the automated tool. Through an automated security verification using the AVISPA (Automated Validation of Internet Security Protocols and Applications) simulation tool, we prove that these protocols are not secure.

Index Terms— authentication protocol, NFC, AVISPA tool, DOS attack, replay attack

1. INTRODUCTION

Near Field Communication (NFC) technology is supported by different modern devices such as smartcard, smart phone and tablet PC. This technology is used in various applications like payment, health care, and access control. In addition, it is one of important technologies in Internet of Things (IoT) [1]. One of the major challenges related to NFC technology in mobile services is security where the communication between the NFC tag and the NFC device is based on radio frequency which is unsecured. In the literature, there are important NFC authentication protocols proposed to securing the communication between different NFC-enabled devices and to achieving the security requirement, such as [2, 3, 4].

The design of authentication protocol for NFC is not sufficient. We should verify the achievement of security properties of the protocol. The use of formal automated tools is the efficient method to attain this objective. One of important formal tools, we cite the AVISPA simulation tool (Automated Validation of internet Security Protocols and Applications) [5] which is developed in 2005 by AVISPA European project. If the security protocol is not secure, AVISPA can simulate the detected attacks.

In 2015, Beak and Youm [6] proposed an authentication protocol for NFC tag based services. The authors present two versions of this protocol depending on treatment of NDEF (NFC Data Exchange Format) messages. Firstly, an NFC tag authentication protocol and the second is a NFC-enabled device authentication protocol. The entities of these protocols are: NFC tag, NFC device, and service provider server (SP Server). In this paper, simulation using AVISPA tool of Beak-Youm protocol is presented for verifying security. Through AVISPA (Automated Validation of Internet Security Protocols and Applications) tool, we prove that these versions are not secure against replay and denial of service attacks. Moreover, we discus causes of these attacks and how avoid them.

The rest of this paper is structured as follows: Section 2 presents main preliminaries. In section 3 we study the NFC tag authentication protocol. The analysis of NFC-enabled device authentication protocol is shown in Section 4. Finally, the paper is finished by a general conclusion.

2. BACKGROUND

In this section we introduce the main preliminaries about the security requirement in NFC authentication protocols, the AVISPA tool, and the intruder model.

2.1. Security requirements

Authentication protocols for NFC tags should satisfy the security requirements as follows:

- *Confidentiality*: The verification that the secret data are never passed on clearly in communication channel which can be spied on.
- *Mutual authentication*: A NFC authentication protocol achieves mutual authentication that is to say; it achieves the server's authentication and the NFC tag's/device's authentication. In the first one, a tag/device has to be

able to confirm that it communicates with the legitimate server. In the last one, the server has to be capable of verifying a correct tag/device to authenticate and to identify an NFC tag/device in complete safety.

- *Denial of service prevention*: The system does not resist denial of service attack if the adversary can block NFC devices' signals or realizes desynchronization between the NFC tag/device and the server, so that they are not correlated in future sessions.

- *Man-In-The-Middle attack resisting*: The intruder could interfere with messages transmitted between a NFC device and a NFC tag by insertion, modification, or deletion, in order to impersonate it later.

- *Replay attack resisting*: The intruder can eavesdrop to the message answer of the tag and to the device. It will broadcast the message listened without modification to the device later.

2.2. AVISPA tool

AVISPA simulation tool is one of important automated tools which are used to validate the security properties of several security protocols in different systems and applications, such as RFID systems [7], NFC technology [3], WSN [8], and IoT technology [9]. It employs four back-ends to tackle validation of cryptographic protocols, and particularity, authentication protocols in our study: OFMC (On-the-fly Model-Checker), CL-ATSE (Constraint-Logic-based Attack Searcher), SATMC (SAT-based Model-Checker) and TA4SP (Tree Automata based on Automatic Approximations for the Analysis of Security Protocols). AVISPA tool can detect the replay and man-in-the-middle attacks. It also can verify two important security properties: secrecy and authentication.

AVISPA provides a language named the High Level Protocol Specification Language (HLPSL) [10] for describing security protocols and specifying their intended security properties, as well as a set of back-ends to formally validate them. HLPSL is a modular, expressive, formal, role-based language, meaning that we specify the actions of each kind of participant in a module, which is called a basic role.

2.3. Intruder Model

To verify an authentication protocol, it is necessary to model the intruder. In other term, we need define its behaviour and limit. On of important existing model, we cite "model Dolev-Yao" [11] which is agreed in AVISPA tool. This intruder model is based on two assumptions that are the perfect encryption and the adversary is the network. Perfect encryption ensures in particular that an intruder can decrypt a message m encrypted with key k if it has the opposite of that key. The second assumption which is "the intruder is the network" means that is, the intruder has complete control over the network. It can modify, interrupt, and intercept transmitted messages between the entities. It also can create new messages from its initial knowledge and the messages received from the entities during protocol runs. The communication between the NFC tag and NFC device is not secured and based on radio frequencies waves. In our analysis, we place the intruder between the NFC tag and NFC device. The adversary can communicate with honest NFC tag as NFC device, and as well as can communicate with honest NFC device as NFC tag.

3. NFC TAG AUTHENTICATION PROTOCOL

In this section, we review the NFC tag authentication protocol and we prove that they are not secure. To describe the studied protocols, we afterward, use the following notations, these are described in Table 1.

Table 1. Notations and descriptions.

Notation	Description
D, T, SP	The device, the tag, and the service provider server respectively
I	the intruder
ID	identifier of a NFC tag of length l
DID	identifier of a NFC device
Rsi	i-th secret value for the NFC tag
Rt	Random value of NFC tag
Rdi	i-th random value for the NFC device
p	Random number for partial ID (l/2 ¡ p ¡ l)
Pid	Partial ID for the NFC tag
$Pdid$	Partial ID for the NFC device
H	One-way hash function
$\|$	Concatenation of two inputs
$\oplus$	Or-exclusif

3.1. Review of the protocol

This protocol is proposed to authenticate the NFC tag prior to read the NDEF messages from tag. In the initialisation phase, the server generates the unique identifier of tag ID and random value Rs_i. Then, the server sends (ID, Rs_i) to the NFC tag through a secure channel. The authentication phase takes place as follows (to see Fig. 1):

- When the NFC device sends the query to the NFC tag, the tag generates a nonce Rt and computes $TReq$ and α, where $TReq = H(ID\|Rs_i)$ and $\alpha = Rs_i \oplus Rt$.

- NFC tag sends $TReq$ and α to the NFC device. It resends the received message to the SP server.

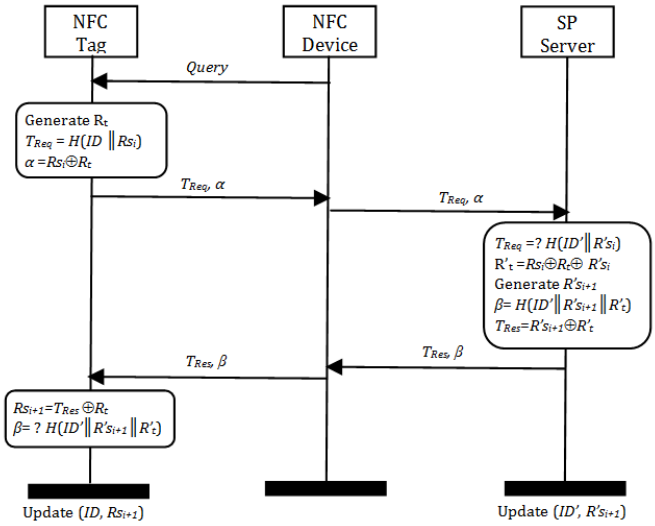


Fig. 1. Schematic diagram of the NFC tag authentication protocol

- From the database, the SP server looks for certain $(ID', R's_i)$ to compute $T'Req$ and make the comparison: $TReq = ?T'Req$. If it is not found, the SP server terminates the session; otherwise it crosses the tag authentication and is considered as legitimate. Then it extract the the value of $R't$ from $\alpha \oplus Rsi$. The server generates a new value of Rs_{i+1} and calculates β and $TRes$, where $\beta = H(ID\|Rs_{i+1}\|Rt')$ and $TRes = R'si_{i+1} \oplus R't$ respectively. SP server sends $TRes$ and β to the NFC device, and then update the shared secret, $(ID', R's_{i+1})$, in the database.
- NFC device resends the received message to the NFC tag.
- The NFC tag obtains Rs_{i+1} by computing $\beta \oplus Rt$. It calculates $\beta' = H(ID\|Rs_{i+1}\|Rt)$ and verify if $\beta' = \beta$. If they are equal, the server authentication is successful; otherwise, the server authentication will fail. The NFC tag updates the secret (ID, Rs_{i+1}). After terminate this step with successfully, the NFC device can read the NDEF message from the legitimate tag.

3.2. Replay attack

After specifying the NFC tag authentication protocol by HLPSL and verifying this protocol using AVISPA tool, it is confirmed that this protocol is UNSAFE. Fig 2 shows the attack trace on NFC authentication protocol using OFMC back-end. It presents messages exchanged between the intruder and the legitimate entities (NFC device and NFC tag). We do not show the server because we assume that the communication device server is secured. In this trace result, i represents the adversary, (d, 3) and (d, 6) represents two different sessions of the device, and (t, 3) represents the tag. The posted information such as: Rt(1) is the instance of the nonce Rt, RSi1(2) and RSi1(3) are two instances of the nonce RSi1.

```
% OFMC
% Version of 2006/02/13
SUMMARY
  UNSAFE
DETAILS
  ATTACK_FOUND
PROTOCOL
  /home/span/span/testsuite/results/NFC1.if
GOAL
  replay_protection_on_aut_tag
BACKEND
  OFMC
COMMENTS
STATISTICS
  parseTime: 0.00s
  searchTime: 0.02s
  visitedNodes: 3 nodes
  depth: 2 plies
ATTACK TRACE
i -> (t,3): start
(t,3) -> i: Rt(1) XOR rsi.h(id.rsi)
i -> (d,3): Rt(1) XOR rsi.h(id.rsi)
(d,3) -> i: Rt(1) XOR RSi1(2).h(id.RSi1(2).Rt(1))
i -> (d,6): Rt(1) XOR rsi.h(id.rsi)
(d,6) -> i: Rt(1) XOR RSi1(3).h(id.RSi1(3).Rt(1))
```

Fig. 2. Attack trace on NFC tag authentication (OFMC beckend)

We describe this attack trace as follows:

1. The intruder launches a session by sending a request to the legitimate tag (t, 3).
2. The NFC tag generates a nonce Rt(1). It computes Rt(1) XOR rsi.h(id.rsi) and sent it. The adversary captures and stores this message.
3. The adversary sends the captured message to the NFC device (d, 3).
4. After verification the tag's authentication, the NFC device computes the message Rt(1) XOR RSi1(2). h(id.RSi1(2).Rt(1)) and the send it. The adversary captures the last one.
5. The intruder launches a new session to communicate with the NFC device (d, 6). It sends the captured message in Msg2 to the NFC device.
6. NFC device authenticates the adversary as legitimate tag. It computes the message Rt(1) XOR RSi1(3). h(id.RSi1(2).Rt(1)) and send it. The intruder captures the last one.

In the replay attack, the messages from one protocol session (i.e., one execution of the protocol) are used in

another session. The main cause of replay attack in this protocol is not to use the nonce Rt in the hash function $TReq = H(ID\|Rs_i)$. In case we change the value of $TReq$ to $H(ID\|Rs_i\|Rt)$, then we avoid this weakness.

3.3. DOS attack

The main aim of this attack is to do the communication between legitimate entities is not correlated. The following is a detailed description of each step:

1. We suppose that the protocol is processing normally until the step of the tag's authentication, which it is successful. Device sends $TRes$, β to NFC tag and updates $R's_i$ by $R's_{i+1}$.

2. The adversary blocks the messages transmitted between D and T and ends the session. In this case, the tag does not update Rsi and it keeps its old value.

3. In the next session, D sends the query message to T.

4. T computes $(TReq, \alpha)$ and sends them to the SP server via D.

5. From the database, the SP server looks for certain $(ID', R's_i)$ to compute $T'Req$ and make the comparison: $TReq$ $=?T'Req$. In this case, the tag's authentication has failed because the received (ID, Rs_i) is different from $(ID, R'si)$ which is stored in the database.

4. NFC-ENABLED DEVICE AUTHENTICATION PROTOCOL

4.1. Review of the protocol

This protocol is designed to authenticate the device prior to overwrite the NDEF messages of the NFC tag by the device. In the initialisation phase, the server generates the unique identifier of device DID and random value Rd_i and share their between the tag and the device. The values of (ID, Rs_i) and (DID, Rd_i) are updated in end of each session. The authentication phase takes place as follows (to see Fig. 3):

- The NFC device generates the nonce p, where p = l/2 ¡ p ¡ l, which is used to compute the partial IDs of the tag and then sends the query and p to the NFC tag.

- The NFC tag calculates $TReq$, where $TReq = H(ID\|Rsi)$, and sends it to the device.

- The NFC-enabled device calculates $DReq$, where $DReq = H(DID\|Rd_i)$. It sends $DReq$, p and $TReq$ to the SP server.

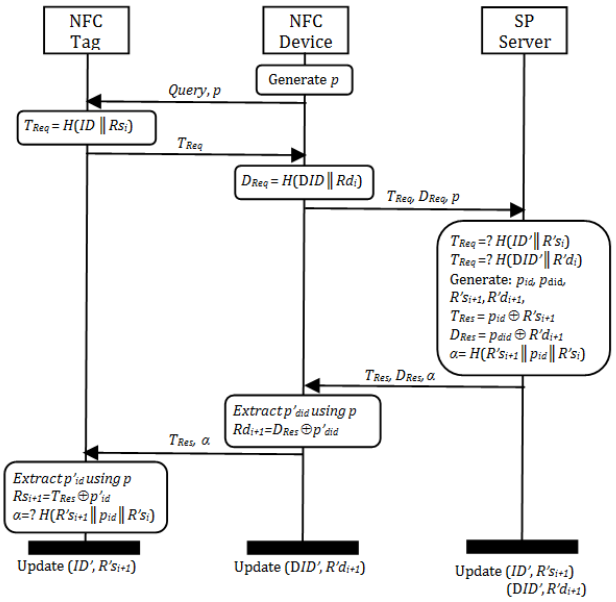


Fig. 3. Schematic diagram of the NFC-enabled device authentication protocol

- From the database, the server finds a set of value for the tag and the device, $(ID', R's_i)$ and $(DID', R'd_i)$ respectively, which are matched with $TReq = H(ID'\|R's_i)$ and $DReq = H(DID'\|R'd_i)$. If match no is found, the server ends the session. On contrary, the server generates the new random numbers, $R's_{i+1}$ and $R'd_{i+1}$. Then, the server extracts the p-bits partial IDs of the tag and the device, pid and $pdid$, which are selected from LSB of each ID. After this, the server calculates $TRes$, $DRes$, and α, where $TRes = R's_{i+1} \oplus pid$, $DRes = Rd_{i+1} \oplus pdid$ and $\alpha = H(R's_{i+1}\|pid\|R's_i)$ respectively. It sends $TRes$, $DRes$ and α to the device. Finally, the server updates the values of shared secrets, $(ID, R's_{i+1})$ and $(DID, R'd_{i+1})$.

- If the device extracts $p'did$ using the random number p. It calculates $DRes \oplus p'did$ to extracts Rd_{i+1}. Then, the device updates the shared secret, (DID, Rd_{i+1}) and transmits $TRes$ and α to the NFC tag.

- The NFC tag extracts $p'id$, using the ramdom number p and calculates $TRes \oplus p'id$ to extracts Rs_{i+1}. Then, the tag calculates $H(Rs_{i+1} \oplus p'id \oplus Rs_i)$ and compares its value with α. If they are equal, the server authentication is successful. Finally, the NFC tag updates the shared secret, (ID, Rs_{i+1}). The legitimate device can overwrite the NDEF messages to the tag after this step.

4.2. Weakness in mutual authentication

AVISPA tool detects an attack on authentication of tag. Fig 4 presents the trace of attack on this protocol with the CL-Atse back-end. We can simplify the description of the attack trace by using Alice-Bob notation as follows:

```
% ATSE
SUMMARY
UNSAFE
DETAILS
ATTACK_FOUND
TYPED_MODEL
PROTOCOL
/home/span/span/testsuite/results/NFC2.if
GOAL
Authentification attack on
(d,t,aut_tag,h(idt.rd))
BACKEND
CL-AtSe
STATISTICS
Analysed: 4 states
Reachable: 2 states
Translation: 0.01 seconds
Computation: 0.00 seconds
ATTACK TRACE
i->(t,7) :start
(t,7)-> i : n13(P)
i->(d,3) :start
(d,3)-> i : n1(P)
i->(t,4) : P(7)
(t,4)-> i : h(idt.rd)
i->(s,9) :h(idt.rd)
(s,9)- >i:
xor(n23(Rsi1),part(idt.P(23))).xor(n23(Rdi1),part
(rs.P(23)))
```

Fig. 4. Attack trace on tag authentication (CL-ATSE back-end)

$$
\begin{aligned}
&\mathrm{I} \longrightarrow \mathrm{T} \quad : \quad Start \\
&\mathrm{T} \longrightarrow \mathrm{I} \quad : \quad p \text{ (instance of nonce)} \\
&\mathrm{I} \longrightarrow \mathrm{D} \quad : \quad Start \\
&\mathrm{D} \longrightarrow \mathrm{I} \quad : \quad p' \text{ (instance of nonce)} \\
&\mathrm{I} \longrightarrow \mathrm{T} \quad : \quad p' \\
&\mathrm{T} \longrightarrow \mathrm{I} \quad : \quad h(idt, rd) \\
&\mathrm{I} \longrightarrow \mathrm{SP} \quad : \quad h(idt, rd) \\
&\mathrm{SP} \longrightarrow \mathrm{I} \quad : \quad pidt \oplus Rsi1, pdid \oplus Rdi1, H(Rsi1 \| pidt \| Rsi)
\end{aligned}
$$

The aim of the intruder in this protocol is to attack the tag's authentication property by using the function h (idt, rd), authentication attack on (d, t, aut_tag, h (idt, rd)). For personify the legitimate tag, the intruder uses the random number p for view that $h(id, rd) = h'(id, rd)$. To satisfy this condition the intruder launches the new session to create a nonce p' then the attack is successful.

We notice that the AVISPA tool also detects an attack on device authentication where the intruder used same technique to realize his objective.

4.3. DOS attack

We use the same principle of DOS attack on NFC tag authentication protocol. In this protocol, there are two secret data updated before the ending of session: Rd_i and Rs_i. When the intruder block the last message between SP and D, the secret data have been updated in the database of the SP. However, the NFC device saves the old values of(DID, Rdi) and the NFC tag saves the old values of (ID, Rsi). In next session, the tag's authentication and device's authentication have failed because the received (Rdi, Rsi) are different from ($R'di$,$R'si$) which are stored in the database.

4.4. Improved protocol

To avoid the attack on tag authentication, we propose to change the value of $TReg$ by adding two nonces p and Rt in the hash function $H(IDt \| Rs_i \| p \| Rt)$. Concerning the attack on device authentication, we change the value of $DReg$ by adding two nonces p and Rt in the hash function $H(DID \| Rd_i \| p \| Rt)$. In addition, the server computes $\beta = (Rd_{i+1} \| p' did \| Rd_i)$ and send it to the device to verify Rd_{i+1}.

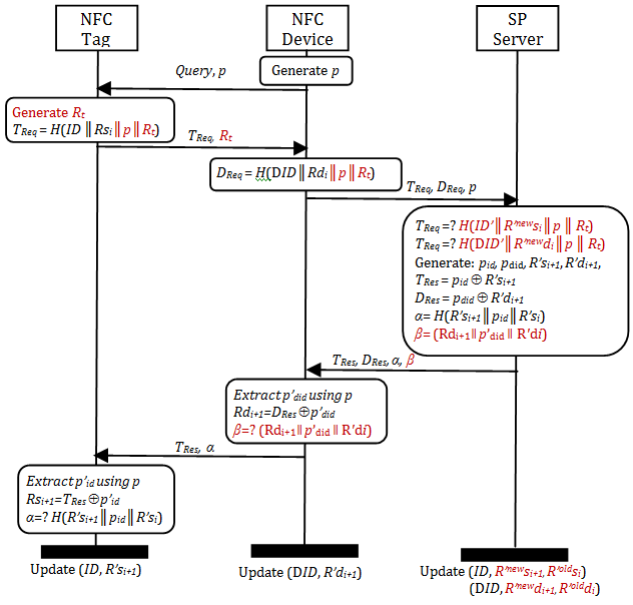


Fig. 5. Schematic diagram of the improved authentication protocol

In DOS attack, the intruder can asynchronize the data that are synchronized during the authentication process. To avoid this problem, we need use the secret synchronisation numbers

in back-end. This approach is used in many authentication protocols (like [12, 13]) and it is effective to resist DOS attacks. For each updated secret datum, we use two numbers, the old value and the new value. The new database contains (ID,Rs_i^{old},Rs_i^{new}) and (DID, Rd_i^{old}, Rd_i^{new}). We suppose that the intruder blocks the last message between SP and D. In the next session, when the server verifies the device's authentication, then the server found a problem because the secret Rd_i^{new} and Rd_i are different. In our protocol, we resolved this problem by using Rd_i^{new}, thus the device's authentication is successful, as well as tag's authentication with Rs_i^{old} and Rs_i^{new}. Fig 5 summarizes our improved protocol.

5. CONCLUSION

Break and Youm proposed two versions of authentication protocol for NFC tag based services. The authors claimed that the two versions of their protocol are effective to prevent existing attacks in NFC systems like, spoofing, DoS, and data modification attacks. In our paper, we presented our vulnerability analysis of these two versions by AVISPA tool. We showed that theses protocols are not secure. Moreover, we proposed the improved NFC-enabled device authentication protocol to prevent the detected attacks. At the improved protocol, we used secret synchronisation values in back-end.

6. REFERENCES

[1] S. H. Shah and I. Yaqoob, "A survey: Internet of things (IOT) technologies, applications and challenges," in *2016 IEEE Smart Energy Grid Engineering (SEGE)*. IEEE, Aug 2016, pp. 381–385.

[2] N. E. Madhoun, F. Guenane, and G. Pujolle, "A cloud-based secure authentication protocol for contactless-nfc payment," in *2015 IEEE 4th International Conference on Cloud Networking (CloudNet)*, Oct 2015, pp. 328–330.

[3] V. Odelu, A.K. Das, and A. Goswami, "SEAP: Secure and efficient authentication protocol for NFC applications using pseudonyms," *IEEE Transactions on Consumer Electronics*, vol. 62, no. 1, pp. 30–38, 2016.

[4] K. Fan, P. Song, and Y. Yang, "ULMAP: Ultralightweight NFC mutual authentication protocol with pseudonyms in the tag for IoT in 5G," *Mobile Information Systems*, vol. 2017, no. 1, pp. 7, 2017.

[5] A. Armando, D. Basin, Y. Boichut, Y. Chevalier, L. Compagna, J. Cuellar, P. Hankes Drielsma, P. C. Heám, O. Kouchnarenko, J. Mantovani, S. Mödersheim, D. von Oheimb, M. Rusinowitch, J. Santiago, M. Turuani, L. Viganò, and L. Vigneron, "The AVISPA tool for the automated validation of internet security protocols and applications," in *International Conference on Computer Aided Verification*. Springer, 2005, pp. 281–285.

[6] J. Baek and H. Y. Youm, "Secure and lightweight authentication protocol for nfc tag based services," in *2015 10th Asia Joint Conference on Information Security*. IEEE, May 2015, pp. 63–68.

[7] N. Chikouche, "Formal analysis of a novel RFID authentication protocol," in *2017 8th International Conference on Computing, Communication and Networking Technologies (ICCCNT)*. IEEE, July 2017, pp. 1–7.

[8] N. Badetia and M. Hussain, "Distributed mechanism for authentication of nodes in wireless sensor networks," in *2017 2nd International Conference for Convergence in Technology (I2CT)*. IEEE, April 2017, pp. 471–474.

[9] R. Amin, N. Kumar, G.P. Biswas, R. Iqbal, and V. Chang, "A light weight authentication protocol for IoT-enabled devices in distributed cloud computing environment," *Future Generation Computer Systems*, vol. 78, pp. 1005 – 1019, 2018.

[10] The AVISPA team, "HLPSL tutorial the Beginner's guide to modelling and analysing internet security protocols," Tech. Rep., AVISPA project, 2006.

[11] D. Dolev and A. Yao, "On the security of public key protocols," *IEEE Transactions on information theory*, vol. 29, no. 2, pp. 198–208, 1983.

[12] A. Maarof, M. Senhadji, Z. Labbi, and M. Belkasmi, "Authentication protocol for securing internet of things," in *Proceedings of the Fourth International Conference on Engineering & MIS 2018*. 2018, ICEMIS '18, pp. 1–7, ACM.

[13] S. Kumari, M. Karuppiah, A.K. Das, X. Li, F. Wu, and N. Kumar, "A secure authentication scheme based on elliptic curve cryptography for iot and cloud servers," *The Journal of Supercomputing*, Apr 2017.

Privacy Analysis of a New Authentication Protocol for Internet of Things

Noureddine Chikouche
Computer Science Department
Mohamed Boudiaf University of M'sila
M'sila, Algeria

***Abstract*—Nowadays, the Internet of Things (IoT) is an important technology that is applied in different applications, such as smart cities, supply chain, digital health monitors, etc. One of the most important challenges related to IoT technology is privacy. Recently, Wang et al. proposed a mutual authentication protocol in IoT environment, it was based on elliptic curve cryptography (ECC) and hash function. Wang et al. claimed that their protocol is secure against different attacks possible in IoT environment. In this paper, we prove that their protocol does not provide untraceability and device anonymity. Moreover, we propose an improved protocol to eliminate the detected weaknesses. Using AVISPA simulation tool, we prove that our improved protocol satisfies security and privacy requirements.**

***Index Terms*—Privacy, Internet of Things, authentication protocol, security**

I. Introduction

The Internet of Things (IoT) is an upcoming technology that permits to interconnect different devices and machines using heterogeneous networks (e.g. radio frequency identification, wireless sensor network, Wi-Fi, etc.) through the bridging and power of the Internet to carry out services to the users, and improve their quality of life. It is applied in various applications, such as smart cities, supply chain, industrial control, digital health monitors, etc. In addition, the importance of IoT appears in the fast augmentation in the number of connected devices to the Internet; the number in 2015 is 25 billion devices and will be 50 billion in 2020.

IoT technology adopts different types of devices and systems, such as RFID tags (Radio Frequency Identification), sensors (WSN: Wireless Sensor Networks), smartphones, NFC mobiles (Near Field Communications), etc. The majority of these IoT devices have restricted computing resources, processing competence, space memory and strict power requirements. With these limitations, there is another important issue, it is the security and privacy of IoT components and the data that is exchanged. The communication between the different IoT entities is unsecured, it requires to choose lightweight cryptographic primitives and design a secured authentication protocol.

In order to have secure authentication protocols, it is important that an authentication protocol for IoT satisfies security and privacy properties, and can resist existing attacks, such as:

- **Data confidentiality**: It means that secrets data can only be read by the authorized entities, the legitimate device and the legitimate server.
- **Mutual authentication**: An authentication protocol achieves mutual authentication, that is to say, it achieves the device's authentication and the server's authentication. In device's authentication, a server has to be capable of verifying a correct device to authenticate and to identify a device in complete safety. In server's authentication, a device has to be capable of confirming that it communicates with the legitimate server.
- **Device anonymity**: This property means that the adversary cannot know the real identity of the device.
- **Untraceability**(or **location privacy**): The untraceability requirement guarantees that the intruder can neither determine who the device is nor distinguish whether two sessions are run by the same device.
- **Desynchronization resilience**: This property specifies for IoT protocols that update a shared secret before ending the protocol. We can define this property as follows: at session (i), the adversary can block or modify the exchanged messages between the server and the device. In the next session, if the authentication process fails, then the device and the server are not correlated and this protocol does not achieve desynchronization resilience.
- **Session key establishment**: A session-key should be launched among a IoT device and a server.
- **Replay attack:** The replay attack is an impersonation attack where the adversary replays or resends precedent exchanged messages between the server and the device in various sessions or in the same session of the protocol to be authenticated as legitimate server or device.
- **MITM attack:** In man in the middle (MITM) attack, the adversary can interfere with messages transmitted between a device and a server by inserting, modifying, inserting, blocking or deleting, in order to impersonate them later.

In literature of authentication protocols for IoT, there are several proposed protocols which used different technologies and various cryptographic primitives (see [1], [2]). The majority of these protocols are oriented to specific systems integrated in Internet of Things, such as RFID systems [3], wireless sensor networks [4], and vehicular ad hoc networks [5].

Machine to Machine Communication (M2M) is a crucial technology that allows tools, machines, and systems, to com-

municate with each other automatically for the realisation of IoT. There are two categories of authentication protocols to secure M2M based on type of communicating machines: the machines are IoT devices (D2D), such as [6], [7]. The second category, the realisation of communication is between IoT devices and server, such as [8]–[11]. In this work, we are interested by the last one.

Our contributions in this paper are listed as follows:

- We analyse the privacy of a recently an authentication protocol for IoT that proposed by Wang et al. [11]. This protocol is based on elliptic curve cryptography (ECC) and hash function. Wang et al. claimed that their protocol is secure against different attacks possible in IoT environment. We prove that their protocol does not provide device anonymity and untraceability.
- To eliminate the detected weaknesses, we propose an improved protocol while maintaining the benefits of the original protocol by using ECDLP and hash function which are lightweight cryptographic primitives.
- By using AVISPA (Automated Validation of internet Security Protocols and Applications) tool [12] to prove that proposed protocol ensures the mutual authentication and session key secrecy.
- We provide security and privacy comparison with recent existing authentication protocols. It illustrates that the proposed protocol is more secure than the studied protocols.

The rest of this paper is structured as follows: section 2 presents the basic concepts of ECC and the adversarial model. Section 3 reviews and analyses the privacy of Wang et al.'s protocol. We present an improved protocol in section 4. In section 5, we analyse the security and the privacy of our improved protocol and compare it with other protocols. Finally, the paper ends with a general conclusion.

II. Background

In this section, we present the primary concepts of elliptic curve cryptography and the capacities of the adversary that agreed in this paper. The list of notations in this paper is shown in Table I.

TABLE I
NOTATIONS

D_i	The embedded device
S	The server
ID_i	Identifier of embedded device
DID_i	Dynamic identifier of IoT device
ID_i^{old}, Id_i^{new}	Two secret synchronization identifiers
N_D	Random number generated by D
N_S, N_{REG}	Random numbers generated by S
K_S	Server's secret key
$\mathbb{F}_q$	Finite field
SK	Session key between D_i and S
G	Generator point of a large order n
CK	Cookie information
X	secret key stored in the server
$ETime$	Expiration time of the cookie
$h(.)$	cryptographic hash function
$\|$	Concatenation of two inputs

A. Elliptic Curve Cryptography

Elliptic Curve Cryptography (ECC) [13] is considered as an approach to public key cryptography based on the hardness problem, namely the elliptic curve discrete logarithm problem (ECDLP). It can be used for asymmetric operations such as key exchange on a channel non-secure or asymmetric encryption.

Let a and b be real numbers. An elliptic curve E over the field of real numbers R is the set of points (x,y) with x and y in R that satisfy the equation $y^2 = x^3 + ax + b$ with the condition $4a^3 + 27b^2 \neq 0$ along with a distinguished point at infinity.

The definition of ECDLP is as follows: given $P, Q \in E(\mathbb{F}_q)$ to find an integer m, if it exists, such that $Q = m \times P$. The solution of this problem is very hard for appropriate parameters [14]. The hardness of ECDLP permitted to develop several cryptographic schemes based on elliptic curves.

ECC is a lightweight primitive that requires less space than other public-key cryptosystems. For example, a 160-bit ECC key offers an equivalent security 1024-bit RSA key.

B. Adversarial model

To verify an authentication protocol, it is necessary to model the adversary. In other term, we need define its behaviour and limit. In Internet of Things technology, the communication between different devices and the server is unsecured, this permits to the adversary to control the exchanged messages. The capabilities of the adversary are as follows:

- eavesdrop on messages passing through the communication channel,
- create new messages from its initial knowledge,
- decrypt ciphertext if it has the secret key,
- communicate with honest devices and honest server,
- compromise the secret data saved in a legitimate device,
- memorise all transmitted messages to use them later,
- employ different primitives and encryption algorithms (e.g. hash function, ECDLP, etc.).

III. Related Works

There are several authentication protocols in IoT technology that based on elliptic curve cryptography (ECC), such as [8]–[11]. Kalra and Sood [8] (KS protocol) proposed a mutual authentication and key agreement protocol for secure communication of IoT devices and cloud servers using Hyper Text Transfer Protocol (HTTP) cookies in context of IoT. The authors claimed the proposed protocol ensures mutual authentication and achieves essential security requirements. KS protocol has been criticized in several papers [9], [10]. Chang et al. [9] pointed out that the KS protocol does not achieve mutual authentication and session key agreement. Subsequently Chang et al. presented an improved protocol to avoid the detected vulnerabilities in the studied protocol. Kumari et al. [10] demonstrated that in the KS protocol it is not possible to realise mutual authentication, session key agreement, and device anonymity. Moreover, it is susceptible to off-line password guessing and insider attacks. Based on

detected flaws of KS protocol, Kumari et al. proposed a new authentication protocol for IoT and cloud servers using elliptic curve cryptography algorithm. Maarof et al. [15] also discussed the security of KS protocol and then showed its weaknesses in mutual authentication, session key agreement and untraceability. They proposed an enhanced protocol to avoid the mentioned attacks, however, it does not resist desynchronization attacks.

In 2017, Wang et al. [11] pointed out a proof that the Chang et al.'s protocol is insecure. The authors showed efficient impersonation attack, where the intruder can impersonate a legitimate server and establish a connection with a device. In addition, Wang et al. were improved upon the Chang et al.'s authentication protocol by removing the password and by changing the calculation method of different transmitted messages.

IV. Wang et al.'s protocol

In this section, we present the IoT system architecture, different phases of Wang et al.'s protocol, and the security analysis of the last one.

A. IoT system architecture

In IoT environment that agreed in studied authentication protocol [11], there are two entities, a set of IoT devices and a server. These entities are communicating via the Internet.

- *IoT device*: It is constrained device that makes part of the Internet and holds characteristics that is overlooked by other Internet nodes. This constrained device can be sensor, smart object, smart device, or actuator. It is quite constrained in code space and processing capabilities and it supports the security functions. The IoT device plays a role of HTTP (Hyper Text Transfer Protocol) client.
- *Server*: The server has the sufficient computational resources and storage space. The server plays a role of HTTP-enabled server (HTTP server), it can communicate with IoT devices (HTTP clients). Before accessing to services in the server, the IoT device and the server realise the mutual authentication between them.

B. Review of Wang et al. Scheme

In 2017, Wang et al. [11] proposed a mutual authentication protocol to connect the trusted server S to several IoT devices D for IoT environment. This protocol is based on ECC using two assumptions, Elliptic Curve Discrete Log Problem (ECDLP) and Elliptic Curve Computational Diffie-Hellman (ECCDH). They consider an elliptic curve to be an additive group $\mathcal{G}$ and G is an element of this group.

The server picks some system parameters: a hash function $h(.)$, a elliptic curve E, a generator G on E and shares them as public parameters. It has a long term secret key X and it is not shared with any other embedded devices. An IoT device D_i selects its unique identifier ID_i.

Wang et al.'s protocol is divided into two phases: the registration phase, and the login and authentication phase (to see Fig. 1).

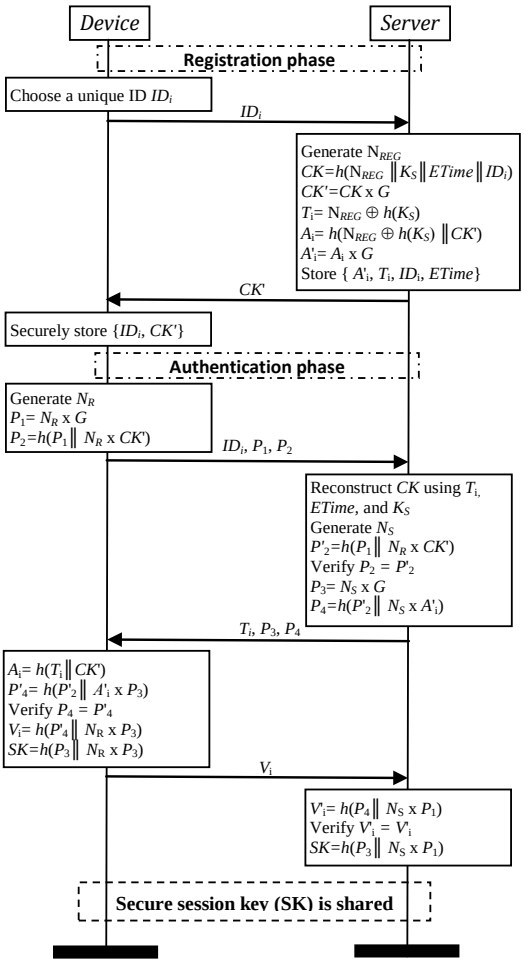


Fig. 1. Illustration of Wang et al. Scheme

1) Registration phase: The registration phase is run in case an IoT device D_i wants to obtain service from the server S. The D_i sends the unique identity ID_i to S. Subsequently, S generates a random number N_{REG} and calculates a cookie $CK = h(N_{REG} \parallel K_S \parallel ETime \parallel Id_i)$ and the cookie point $CK' = CK \times G$. Then, S calculates $T_i = N_{REG} \oplus H(K_S)$,$A_i = h(N_{REG} \oplus H(K_S) \parallel CK')$ and the point $A'_i = A_i \times G$

The server stores $\{ID_i, A'_i, T_i, ETime\}$ in its database. Then, the server sends the cookie point CK' to the corresponding IoT device through a secure channel where CK' is strictly confidential. Then, the stored data in permanent memory of IoT device are $\{ID_i, CK'\}$.

2) Login and authentication phase: The authentication phase takes place as follows:

- The IoT device D_i generates a random number N_D and calculates the values of P_1 and P_2, where $P_1 = N_D \times G$ and $P_2 = H(P_1 \parallel N_D \times CK')$. D_i sends $\{ID_i, P_1, P_2\}$ to the server.
- After receiving authentication message from D_i, S retrieves the stored record associated with ID_i from the

database. It verifies the value of P_2, then it selects a random number N_S and computes P_3 and P_4 where $P_3 = N_S \times G$ and $P_4 = H(P_2' \parallel N_S \times A_i')$. S sends $\{T_i, P_3, P_4\}$ to the IoT device D_i

- D_i verifies the value of P_4 by reconstructing A_i from T_i and CK'. If they are equal, the device calculates the values of V_i and the session key SK where $V_i = H(P_4' \parallel N_D \times P_3)$ and $SK = H(P_3 \parallel N_D \times P_3)$. Finally, D_i sends V_i to the server.
- S computes the values of V_i and SK by considering the equality $N_{ED} \times P_3 = N_S \times P_1 = N_{ED} \times N_S \times G$. The value of SK is the secret key during this session.

C. Privacy analysis of Wang et al.'s protocol

1) Violation of device anonymity: One of capabilities of the adversary is to eavesdrop on device/server communications. In Wang et al.'s protocol, the identifier's device ID_i is passed clearly in the communication device-to-server. In addition, Wang et al. did not use any mechanism to identity-protection for device (such as hash function, random number, signature, etc.),this implies that the identity of the device is not protected. Therefore, the adversary knows the real identifier of the IoT device by intercepting the first message in authentication protocol. Then, this protocol does not satisfies device anonymity.

2) Violation of untraceability: The principal method of the traceability attack is that the adversary can trace the IoT device via the messages captured from the communication channel. Unfortunately, in authentication phase of Wang et al.' protocol, the value of identifier's device ID_i is static in all sessions and is transmitted without any protection. This implies that the adversary can follow the trace of the IoT device. Thus, the Wang et al. authentication protocol does not achieve untraceability.

V. Improved protocol

In protocol proposed by Wang et al., there are two major weaknesses: it cannot resist traceability attack and does not confirm anonymity. Our improved version of Wang et al.'s protocol is shown in Fig. 2.

In registration phase, we add the synchronization data for device's identifier ID_i^{old} and ID_i^{new}, and initialise them by the value of ID_i. Then, database of the server contains $\{ID_i, Id_i^{old}, Id_i^{new} A_i', T_i, ETime\}$. The device stores $\{DID_i, CK'\}$ where DID_i is a dynamic identifier and we initialise it by ID_i.

The authentication phase takes place as follows:

- The IoT device D_i generates a random number N_D and calculates the values of P_1, P_2, where $P_1 = N_D \times G$ and $P_2 = H(P_1 \parallel N_D \times CK')$. D_i sends $\{DID_i, P_1, P_2\}$ to the server.
- After receiving the previous message from D_i, S retrieves the stored record associated with DID_i (either ID_i^{old} or ID_i^{new}) from the database. It verifies the value of P_2, then it selects a random number N_S and computes P_3 and P_4 where $P_3 = N_S \times G$ and $P_4 = h(P_2' \parallel N_S \times A_i')$. Before sending $\{T_i, P_3, P_4\}$ to the IoT device D_i, the server updates the values of ID_i^{old} and , Id_i^{new} as follows: the server updates the values of $ID_i^{old} = Id_i^{new}$ (only in case the matched $DID_i = Id_i^{new}$) and $ID_i^{new} = h(DId_i \parallel (P_1 \times N_S))$.
- D_i verifies the value of P_4 by reconstructing A_i from T_i and CK'. If are equal, the device calculates the values of V_i and the session key SK where $V_i = H(P_4' \parallel N_D \times P_3)$ and updates $DID_i = h(DId_i \parallel (P_3 \times N_D))$. Then, D_i computes the key session $SK = h(N_D \times P_3 \parallel DID_i)$. Finally, D_i sends V_i to the server.
- S computes the values of V_i and SK by considering the equality $N_D \times P_3 = N_S \times P_1 = N_D \times N_S \times G$. The value of $SK = h(N_D \times P_3 \parallel Id_i^{new})$ is the secret key during this session.

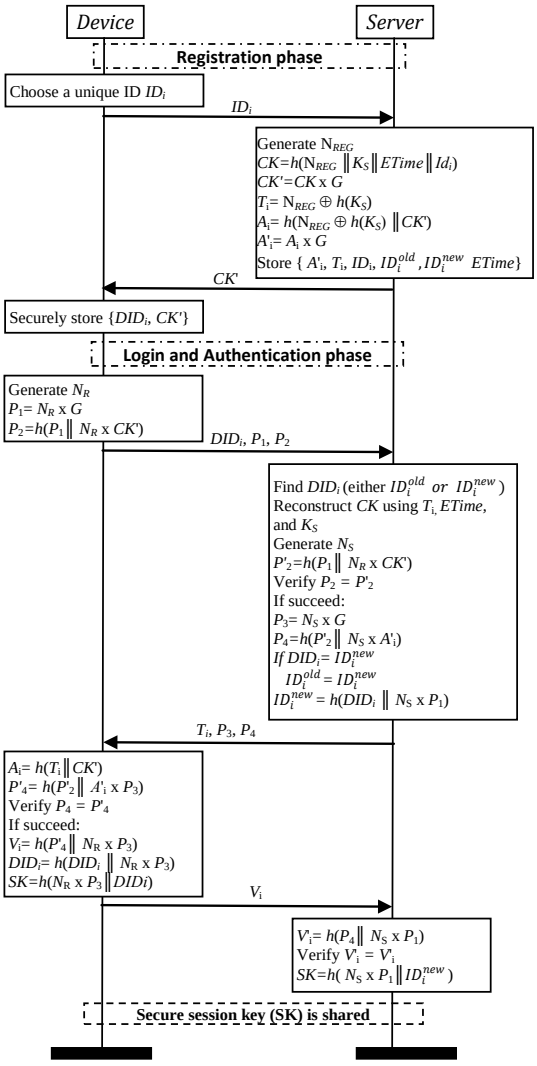


Fig. 2. Illustration of improved protocol

VI. Security and privacy analysis of improved protocol

This section highlights an automated and informal security and privacy analysis of our protocol.

A. Automated security analysis

AVISPA (Automated Validation of internet Security Protocols and Applications) tool [12] is one of the most important automated tools which are used to validate the security properties of several security protocols in different systems and applications, such as RFID systems [16], WSN [17], and IoT technology [18]. It employs four back-ends to tackle validation of cryptographic protocols, and particularity, authentication protocols in our study: OFMC (On-the-fly Model-Checker), CL-ATSE (Constraint-Logic-based Attack Searcher), SATMC (SAT-based Model-Checker) and TA4SP (Tree Automata based on Automatic Approximations for the Analysis of Security Protocols). Among these back-ends, OFMC and CL-ATSE can verify protocols requiring the operator or-exclusive (xor). AVISPA tool can detect the replay and man-in-the-middle attacks. It also can verify two important security properties: the secrecy and the authentication.

```
SUMMARY
  SAFE

DETAILS
  BOUNDED_NUMBER_OF_SESSIONS
  UNTYPED_MODEL

PROTOCOL
/home/span/span/testsuite/results/Improved.if
GOAL
  As Specified

BACKEND
  CL-AtSe
STATISTICS

 Analysed   : 346 states
  Reachable  : 87 states
  Translation: 0.02 seconds
  Computation: 0.22 seconds
```

Fig. 3. Verification result of improved protocol

AVISPA provides a language named the High Level Protocol Specification Language (HLPSL) [19] for describing security protocols and specifying their intended security properties, as well as a set of back-ends to formally validate them. HLPSL is a modular, expressive, formal, role-based language, meaning that we specify the actions of each kind of participant in a module, which is called a basic role.

When a security property of the input specification protocol not achieved then AVISPA tool outputs a warning message (UNSAFE) with the detail of attack trace. In another case, if the protocol achieves security properties, it outputs a message (SAFE). Figure 3 shows that our protocol has been found to be safe and that no attacks have been detected. Thus this protocol resists replay attacks and man-in-the-middle attacks. It also satisfies mutual authentication and the secrecy of secret data (N_D and N_S). One can thus deduce that the diagnostic of AVISPA tool for our protocol is secure.

B. Informal security and privacy analysis

This sub-section analyses the security features of the improved protocol and shows that all security and privacy requirements presented in Table II are assured in our improved protocol.

TABLE II
Security and privacy comparison

	[9]	[11]	[15]	Our protocol
Mutual Authentication	N	Y	Y	Y
Device anonymity	N	N	Y	Y
Untraceability	N	N	Y	Y
Desynchronization resilience	-	-	N	Y
Session key establishment	Y	Y	Y	Y
Resisting Reply attack	Y	Y	Y	Y
Resisting MITM attack	N	Y	Y	Y

"Y" means the property is achieved.
"N" means the property is not achieved.
"-" means the property is not discussed.

1) Data confidentiality: The secret and sensible data in our authentication protocol are: (CK', N_D, N_S). To protect them we used two mechanisms: an encryption algorithm based ECDLP and a robust cryptographic hash function. On intercepting the messages (P_1, P_2) or (P_3, P_4) or V_i, the adversary cannot obtain any secret data. It is hard to obtain the random numbers (N_D, N_S) and the secret data CK', because we use a secure cryptographic primitives and they are not send clearly over the insecure channel.

2) Mutual authentication: In the improved protocol, S firstly verifies the validity of DID_i. After that, S authenticates D_i by checking whether P_2=P_2'. On the other hand, D_i authenticates S by verifying whether P_4=P_4' and compute a valid session key, SK. After S receives V_i, it can verify the equality V_i=V_i' to authenticate D_i and to establish the session key, SK. Therefore, our improved protocol ensures mutual authentication.

3) Device anonymity: The IoT device stores DID_i in its memory. At the end of each session, the device updates the value of DID_i, the new one is $h(DID_i \parallel (N_D \times N_S \times G))$, which is shared with the server. The adversary cannot acquire the last dynamic identifier DID_i used in the previous sessions. Thus the proposed protocol satisfies device anonymity.

4) Untraceability: In the protocols [8] [9] [11], the value of identifier ID_i is static in all sessions that means these protocols do not preserve the untraceability. In our protocol, we use the mechanism of dynamic identifier where ID_i is updated in each session $DID_i = h(DId_i \parallel (P_3 \times N_D))$ = $h(DID_i \parallel (N_D \times N_S \times G))$ where the random numbers (N_D,N_S) are protected by using ECC and a secure hash function. With these different mechanisms of protection the adversary cannot flow the trace of target device. So, the proposed protocol ensures untraceability property.

5) Desynchronization resilience: The updating secret shared data in each session is one important mechanism to resist location tracking attack. Unfortunately, this mechanism poses a security problem called desynchronization attack where the adversary can asynchronize the data that are synchronized during the authentication process. To avoid this weakness, we used two synchronised numbers for the identifier, ID_i^{old} and ID_i^{new} stored in the database of the server. We suppose that the adversary blocks the last message in authentication protocol. In the next session, when the server verifies the device's authentication, then the server find a problem because the values of ID_i^{new} and ID_i are different. In our protocol, we resolved this problem by using the old identifier ID_i^{old}, thus the device's authentication is successful.

6) Session key establishment: The session key SK that computed in end of authentication protocol is used to encrypt the secret information during send messages between the entities using a symmetric-key encryption algorithm. SK is changed in each session of communication. In our protocol, D_i and S share the session key $SK = h(N_D \times N_S \times G \parallel DID_i)$. N_S and N_D are two random nonces shared between D_i and S only. From these reasons, the proposed protocol provides session key establishment.

7) Replay attack: Random numbers is mechanism used in authentication protocols to protect them against replay attacks. In our work, we used random numbers where all exchanged messages are involved freshly by generated random numbers (N_S,N_D) in every session. Thus, an adversary cannot replay eavesdropped messages from previous sessions.

8) MITM attack: The adversary cannot obtain the secret data and the session key because all secret data are encrypted by ECC public-key encryption scheme and protected by a secure cryptographic hash function. However, the session key is generated in the end of run of the authentication protocol and not transmitted in communication channel. We suppose that adversary is of type active adversary, then it can modify the exchanged messages. When it modifies the values of the transmitted messages P_1, P_2, P_3, P_4 and V_i by different values P_1', P_2', P_3', P_4' and V_i'. Consequently, the authentication will be unsuccessful. Therefore, the improved protocol is secure against the man-in-the-middle attack and the adversary cannot cheat the legal entities.

VII. Conclusion

Recently, Wang et al. proposed a mutual authentication protocol for IoT based on elliptic curve cryptography. In this paper, we have analysed the privacy of this protocol. The results of our analysis showed that Wang et al.'s authentication protocol cannot resist traceability attack and does not ensure device anonymity.

Moreover, we proposed the improved version of Wang et al.'s protocol to prevent the described attacks. At the improved protocol, we used secret synchronisation values in back-end and we updated the value of the device's identifier before ending the session. Using automated and informal analysis, we proved that our improved protocol is secure.

References

[1] M. A. Ferrag, L. A. Maglaras, H. Janicke, J. Jiang, and L. Shu, "Authentication protocols for internet of things: A comprehensive survey," *Security and Communication Networks*, vol. 2017, 2017.

[2] D. J. Wu, A. Taly, A. Shankar, and D. Boneh, *Privacy, Discovery, and Authentication for the Internet of Things*. Cham: Springer International Publishing, 2016, pp. 301–319.

[3] S. F. Aghili, M. Ashouri-Talouki, and H. Mala, "Dos, impersonation and de-synchronization attacks against an ultra-lightweight RFID mutual authentication protocol for iot," *The Journal of Supercomputing*, Sep 2017.

[4] P. Chandrakar and H. Om, *A Secure and Privacy Preserving Remote User Authentication Protocol for Internet of Things Environment*. Singapore: Springer Singapore, 2017, pp. 537–551.

[5] P. Vijayakumar, V. Chang, L. J. Deborah, B. Balusamy, and P. Shynu, "Computationally efficient privacy preserving anonymous mutual and batch authentication schemes for vehicular ad hoc networks," *Future Generation Computer Systems*, vol. 78, no. Part 3, pp. 943 – 955, 2018.

[6] F. K. Santoso and N. C. Vun, "Securing iot for smart home system," in *Consumer Electronics (ISCE), 2015 IEEE International Symposium on*. IEEE, 2015.

[7] N. Li, D. Liu, and S. Nepal, "Lightweight mutual authentication for IoT and its applications," *IEEE Transactions on Sustainable Computing*, vol. 2, no. 4, pp. 359–370, 2017.

[8] S. Kalra and S. K. Sood, "Secure authentication scheme for iot and cloud servers," *Pervasive and Mobile Computing*, vol. 24, pp. 210–223, 2015, special Issue on Secure Ubiquitous Computing.

[9] C.-C. Chang, H.-L. Wu, and C.-Y. Sun, "Notes on secure authentication scheme for IoT and cloud servers," *Pervasive and Mobile Computing*, vol. 38, no. Part 1, pp. 275–278, 2017.

[10] S. Kumari, M. Karuppiah, A. K. Das, X. Li, F. Wu, and N. Kumar, "A secure authentication scheme based on elliptic curve cryptography for iot and cloud servers," *The Journal of Supercomputing*, Apr 2017.

[11] K.-H. Wang, C.-M. Chen, W. Fang, and T.-Y. Wu, "A secure authentication scheme for internet of things," *Pervasive and Mobile Computing*, vol. 42, pp. 15–26, 2017.

[12] A. Armando, D. Basin, Y. Boichut, Y. Chevalier, L. Compagna, J. Cuellar, P. H. Drielsma, P. C. Heám, O. Kouchnarenko, J. Mantovani, S. Mödersheim, D. von Oheimb, M. Rusinowitch, J. Santiago, M. Turuani, L. Viganò, and L. Vigneron, "The AVISPA tool for the automated validation of internet security protocols and applications," in *International Conference on Computer Aided Verification*. Springer, 2005, pp. 281–285.

[13] I. F. Blake, G. Seroussi, and N. P. Smart, *Elliptic Curves in Cryptography*. Cambridge University Press, 1999.

[14] D. Hankerson, A. J. Menezes, and S. Vanstone, *Guide to elliptic curve cryptography*. Springer Science & Business Media, 2006.

[15] A. Maarof, M. Senhadji, Z. Labbi, and M. Belkasmi, "Authentication protocol for securing internet of things," in *Proceedings of the Fourth International Conference on Engineering & MIS 2018*, ser. ICEMIS '18. ACM, 2018, pp. 29:1–29:7.

[16] M. EslamnezhadNamin, M. Hosseinzadeh, N. Bagheri, and A. Khademzadeh, "A secure search protocol for lightweight and low-cost RFID systems," *Telecommunication Systems*, vol. 67, no. 4, pp. 539–552, Apr 2018.

[17] N. Badetia and M. Hussain, "Distributed mechanism for authentication of nodes in wireless sensor networks," in *2017 2nd International Conference for Convergence in Technology (I2CT)*. IEEE, April 2017, pp. 471–474.

[18] R. Amin, N. Kumar, G. Biswas, R. Iqbal, and V. Chang, "A light weight authentication protocol for IoT-enabled devices in distributed cloud computing environment," *Future Generation Computer Systems*, vol. 78, pp. 1005 – 1019, 2018.

[19] T. A. team, "HLPSL tutorial the Beginner's guide to modelling and analysing internet security protocols," AVISPA project, Tech. Rep., 2006.

Approach Management Application in Cloud Computing: Runtime vs Docker

1st Asmaa Aouat
University of Oran1 Ahmed Ben Bella
Laboratory of parallel, embedded architectures and high performance

2nd El Abbassia Deba
University of Oran1 Ahmed Ben Bella
Laboratory of parallel, embedded architectures and high performance

3rd Abou El Hassan Benyamina
University of Oran1 Ahmed Ben Bella
Laboratory of parallel, embedded architectures and high performance

***Abstract*—Cloud Computing refers to a set of technologies and systems that provide various types of resources (computing, storage, software, etc.) on demand, through the Internet or Intranet. Thanks to these advantages many Cloud providers are available and is increasing even more. The development and deployment of applications in the Cloud offers a new scientific challenge in terms of expression and taking into account variability. Indeed, Cloud Computing is based on heterogeneity principles, which allows many configuration and sizing choices. The purpose of our work is to provide a tool that automates the process of deploying applications in a cloud environment based on the script approach, to configure and provision applications to be deployed in the cloud.**

***Index Terms*—Script approach, Runtime, Container, Docker, Command Line Interface, Provider Cloud, Automation, Metrics.**

I. Introduction

The industrial Internet revolution has acquired the current potential through three industrial revolutions: IoT, Big Data and Cloud Computing. With these technologies, processing and analysis of large data will become a cloud service and provide significant opportunities to improve plant productivity and provide better products in smart plants [5].
Many individuals and organizations have chosen to move their servers or applications to a cloud environment in order to optimize the use of their IT infrastructure, scale-up, high availability, etc... Thus, the exploitation of infrastructure resources in a shared or pooled environment generates cost savings and increased performance. As well as organizations must master redeployment mechanisms for the implementation of fault-tolerant requirements for cloud services against hardware failures and disasters.
Cloud providers highlight the main problem of technological inconsistency for procurement between providers, for example it is difficult to use the advantages of each provider in parallel to satisfy all customer needs (avoid breakdowns, available in all geographical areas, reasonable cost, availability of services). The result of this is vendor lockout, so a software developer must master the different deployment processes for each cloud provider in order to exploit the advantages of each provider.
In addition to the general introduction and conclusion, this document contains five sections. The second section introduces the main tools in the context of deploying applications in the cloud.The third section discusses the implementation technologies for automatic application deployment, the fourth section is a conceptual elaboration of the solution adopted for automatic deployment. The fifth section is an experimentation and evaluation of the product described in this manuscript.

Identify applicable funding agency here. If none, delete this.

II. Related work

This section will be dedicated to the presentation of existing solutions in the field of configuration and deployment of applications in the cloud. Existing solutions can be complete environments, tools or plugins.

A. Non-modelled solutions

Current solutions for configuring and deploying applications in the cloud adopt different approaches, such as scripting, workflow, etc. Among these solutions:

SALOON is a variability expression and decision support software framework for configuring and scaling applications to be deployed in the cloud. Based on ontologies and MCs (Characteristics Models), it takes into account the technical and non-functional aspects of the application to find a cloud

provider that best matches the configuration of the application [7].
The European Cloud4SOA research project offers a PaaS platform that provides a solution for developing and managing applications for a multi-cloud environment. It introduces three-dimensional semantic interoperability, which aims to capture any type of interoperability conflict that occurs at the PaaS layer level [4].

The European research project mOSAIC offers an API and a free PaaS platform to develop and deploy applications "it does not require the direct intervention of the application developer" for a multi-Cloud environment. They focus on abstraction for application developers and the state can easily activate users to obtain the desired application features (such as scalability, fault tolerance, QoS, etc.) [6].

B. A modelled solution

A modeled solution for configuring and deploying applications in the cloud can be defined as a solution that drives a model-driven engineering-focused configuration and deployment process. Among the solutions that adopt the model-driven approach:

Franklin's solution is based on models for the automatic deployment of software on cloud computing. This solution only requires the developer to have knowledge about the access key and the name of the service provider, as the specific details are distracted. The objective is to deploy the software to a higher level of abstraction and reduce human effort and time spent on task deployment, as the model-based approach is a better way to increase developer productivity [8].
MODAClouds: This is a European project aimed at providing methods, a decision support system, a free IDE and an execution environment for high-level design and automatic deployment of applications in a multi-cloud environment while ensuring QoS quality of service [1].

III. Background

In this section we develop the technologies used to develop a tool for configuring and automatically deploying applications on Cloud Computing.

The NIST report [3] stated that multi-cloud can be used in series when an application or service is moved from one cloud to another or when services hosted on different clouds are used simultaneously. The simplest scenarios are migrations from a private cloud application to a public cloud (for serial use) or an application that uses multiple services hosted in different public clouds (for simultaneous use). The reasons why resources and services from multiple clouds are needed are diverse [2].

Deployment is defined according to C. Szyperski as the step of preparing a component for installation in a specific environment. C. Szyperski explicitly states that deployment (i.e., preparation) is the same as filling in the parameters of a deployment descriptor [9].

We will now present the steps that precede and follow this deployment phase as shown in Figure1. This will allow us to clarify where this deployment phase is located in the software life cycle and what its scope is. The step before deployment is acquisition. This is the step of obtaining a software component. C. Szyperski specifies that any acquired component is deployable. This means that a component proposed for acquisition is a deliverable executable by a physical or virtual machine. More precisely, in [9], the author emphasizes that any component must be a deployment unit. It then defines a deployment unit as an executable deliverable in an execution environment, without a human needing to intervene to modify the component to make it effectively installable and ready to run. Installation is the step that immediately follows deployment. It makes a component available on a particular site (host), in a particular environment. It should be noted that this installation step is often automated. Finally, the installation step is followed by the Loading step, which consists in starting the execution of a component in a particular execution context. Most

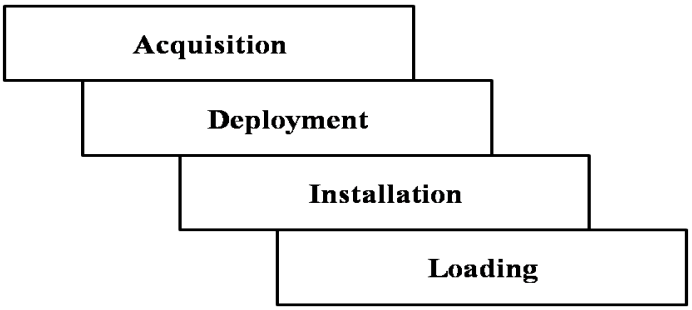


Fig. 1. Deployment phase and its context according to C. Szyperski

cloud providers provide a command line interface (CLI). CLIs allow interaction between the user and the provider where communication between them takes place in text mode (console) by typing instruction lines into a terminal to ask the provider to perform certain tasks. Most cloud providers support many runtime contexts that are used to deploy applications. Providers allow developers to deploy their applications either via runtimes, i.e. programming languages including Java, Javascript, PHP, Python, Go, Node.js, etc. or via containers using Docker open source technology. Developers can also deploy their applications directly from a traditional virtual environment such as the OpenStack Infrastructure, which enables them to run and manage virtual machines in the cloud.

It is important to note that deployment with containers

and virtualization must be performed by qualified personnel.

A container is a virtual envelope that allows you to package an application with all the elements it needs to work: source files, libraries, tools and files. . They are packaged into a coherent package and ready to be deployed on a server and its operating system (OS). Unlike server virtualization, the container does not integrate the OS, it is directly based on the operating system of the server on which it is deployed [10].

Docker is the global platform for software containers, Docker offers the possibility to test and deploy applications on any (local machine, private or public cloud etc...). This technology is based on the use of images to create containers [10].

IV. Automatic deployment approach

In order to deploy any application on cloud computing automatically, we proposed a script-based approach. The first step in this approach is to check the installation and install the tools for interaction with Cloud providers (CLI) if not. The second step includes the declaration of dependencies (packages and libraries) of the application. The third step generates configuration files according to two criteria: the type of application and the selected execution context. The configuration file generation step differs between the two execution contexts since only one configuration file is required for deployment in the docker execution context, but one configuration file for each provider is required for deployment in the runtimes execution context. The multitude of configuration causes the division of the third step into two sub-steps. The configuration step is able to "know each other" and adapt with the programming language with which the application is written in an autonomous way [1]. Once the configuration file is generated, the final step remains to run the application on the Cloud Computing. The steps of the approach are shown in Figure 2.

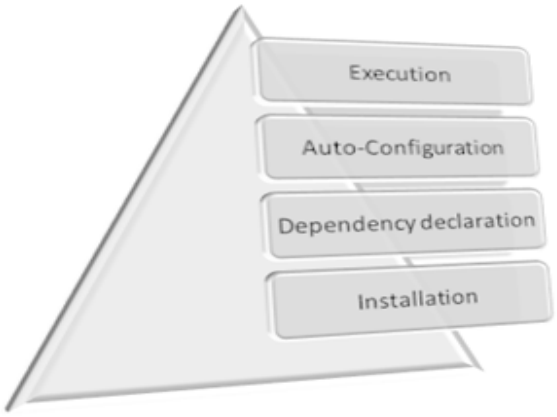


Fig. 2. Steps of the approach

V. Implementation

Based on the approach proposed in the previous section, we have implemented an automatic deployment tool that works seamlessly with different cloud computing providers. The implemented tool allows web applications to be deployed on Cloud Computing. Our deployment tool allows the user to select a cloud provider and the execution context they want to use.

Our deployment tool allows the user to select a cloud provider and the execution context they want to use. Knowing that it offers deployment on three cloud providers: Heroku, IBM Bluemix and Pivotal. The overall architecture of the tool is illustrated in Figure 3.

Our automatic deployment tool can be thought of as a

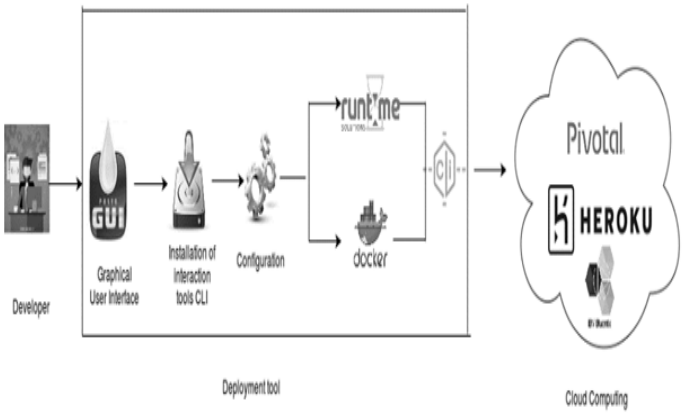


Fig. 3. Architecture of the tool

deployment process that groups together a sequence of phases or steps to execute. The process is illustrated by the sequence diagram in the Figure 4,5 and 6; several messages are exchanged during deployment, the exchange of messages between the developer, the system (our tool) and the provider. In order to explain the deployment process, two sequence diagrams will be cited and detailed:

Especially in step 1 of the deployment sequence diagram in Figure 4, the developer launches the tool (system). Then the developer selects one of the three providers offered. In step 3, an authentication form is displayed. Subsequently the developer seizes his coordinates to authenticate. In step 4 the developer chooses an application to be deployed and the execution method (runtime, docker). Subsequently, the deployed application becomes accessible from a web browser. Specifically in Step 1 of the Installation and Configuration sequence diagram is illustrated in Figure 5, the developer launches the tool (system) and chooses a provider. In step 3, the system verifies the presence of interaction tools between the user and the chosen provider. It is important to note that each provider offers its own CLI. So, if it is not installed then it will install it otherwise the system will update it.

Before deploying the applications on the providers with containers environment, it is necessary of dockerizing the application. Thus for dockerizing an application, it is necessary to follow the diagram of Dockerization sequence.

In particular in stage 1 of the diagram of sequence Dockerization is illustrated in Figure 6, it is necessary to install Docker. Then charged the basic image. In stage 3, the system must create the file dockerfile to build our own image. The authority of our own image is a container. Once the container is ready, one can deploy the application on any provider.

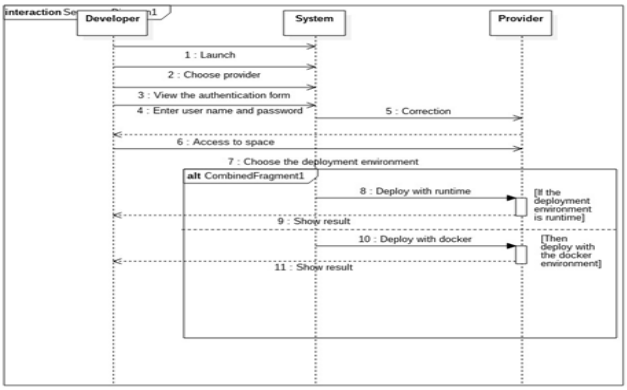


Fig. 4. Sequence diagram for deployment

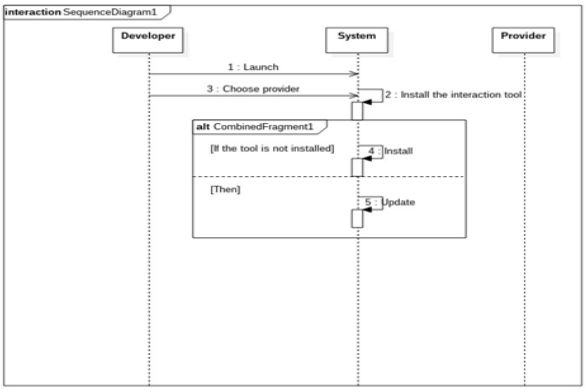


Fig. 5. Sequence diagram for Installation and configuration

VI. Evaluation

In this section we present an experiment based on three objective evaluation measures. The goal behind this experimentation is the evaluation, validation and improvement of our tool in the next works. The experiment aims to analyze and discuss the deployment results using both runtimes and container environments, we analyzed our tool according to 4 evaluation metrics: reliability, portability, time consumed and space used.

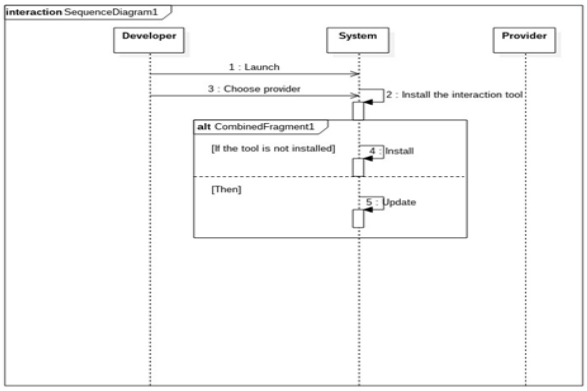


Fig. 6. Sequence diagram for Dockerization

Reliability metrics: Based on the tests performed and shown in Figure 7, we found that containers are more reliable than runtimes because the runtimes environment requires the use of the same version of construction packages used for development (dependencies) as containers that carry application dependencies.

Portability metric: The requirement to use the same version

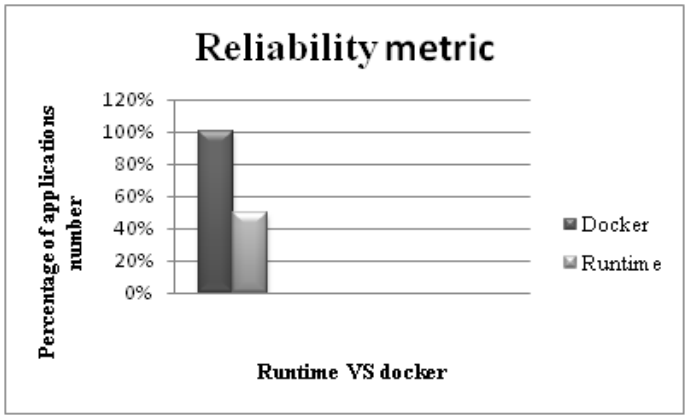


Fig. 7. Reliability metric

of construction packages between the provider and the targeted application for deployment presents an obstacle to portability. So, an application can work on one supplier but on another ”see Figure 8”.

Used space metric: The space used aims to compare between the space reserved at the Cloud provider for deployment in both environments. Figure9 shows that the space allocated in the case of containers is larger than the runtimes due to the size of the base images used.

Consumed time metric: The time consumed in the case of containers is higher than the runtimes because of the size of the data transmitted to the provider (Upload) ”see Figure 10”.

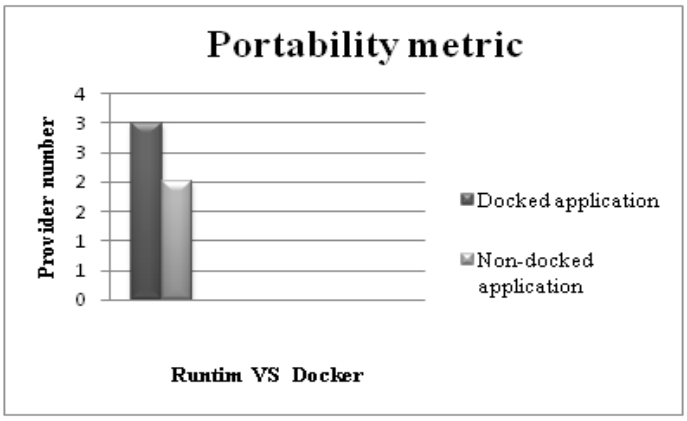


Fig. 8. Portability metric

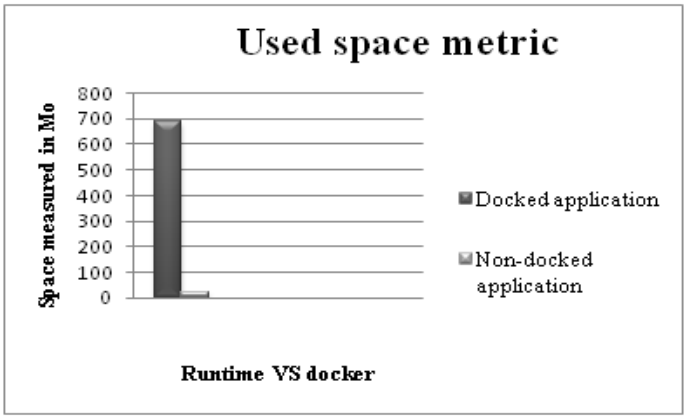


Fig. 9. Used space metric

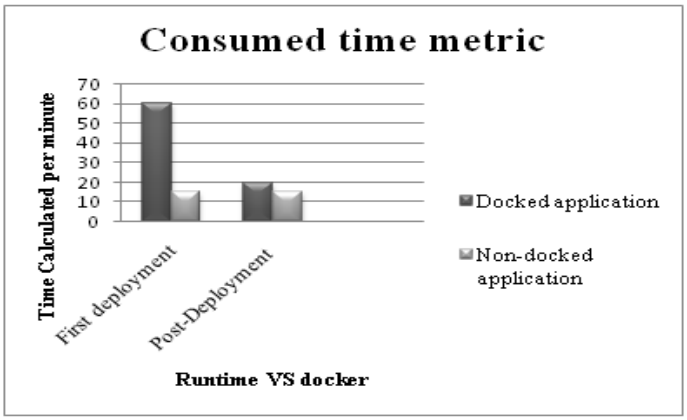


Fig. 10. Consumed time metric

VII. Conclusion

The objective of our project is to reduce the developer's workload, the cost of deployment at the "time and effort" level and also to offer the means to use Cloud Computing resources to deploy applications and make them accessible to audiences. To this end, we have proposed a tool that facilitates the developer's task compared to traditional deployment by using two types of open source services (runtimes and container). The tool developed reduces the risk of error during the deployment process in the generation of the configuration file and the deployment phases.

Our tool offers features that offer many advantages and some limitations:

In order to achieve an automatic deployment, we generated the configuration files automatically, knowing that each provider offers its own configuration file template. The automatic deployment of applications using container technology (Docker) highlights the criterion of application portability between providers. Knowing that this criterion is not yet being radically verified by the Cloud Computing community.

With regard to improving the results of our work, several perspectives can be considered:

Experimentation of applications that contain services such as database services or artificial intelligence services. Experiment with other types of applications such as mobile and IoT applications. Use of virtualization-based execution context to gain more freedom over the operating system and resources exploited in the cloud.

References

[1] Bicevskis, J., Bicevska, Z., §§ & Oditis, I. (2016, July). Self-management of information systems. In International Baltic Conference on Databases and Information Systems (pp. 167-180). Springer, Cham.

[2] Dearle, A. (2007, May). Software deployment, past, present and future. In 2007 Future of Software Engineering (pp. 269-284). IEEE Computer Society.

[3] Hogan, M., Liu, F., Sokol, A., §§ & Tong, J. (2011). Nist cloud computing standards roadmap. NIST Special Publication, 35, 6-11.

[4] Kamateri, E., Loutas, N., Zeginis, D., Ahtes, J., D'Andria, F., Bocconi, S., ... §§ & Tarabanis, K. A. (2013, September). Cloud4soa: A semantic-interoperability paas solution for multi-cloud platform management and portability. In European Conference on Service-Oriented and Cloud Computing (pp. 64-78). Springer, Berlin, Heidelberg.

[5] Li, J. Q., Yu, F. R., Deng, G., Luo, C., Ming, Z., §§ & Yan, Q. (2017). Industrial Internet: A Survey on the Enabling Technologies, Applications, and Challenges. IEEE Communications Surveys §§ & Tutorials.

[6] Moscato, F., Aversa, R., Di Martino, B., Fortiş, T. F., §§ & Munteanu, V. (2011, September). An analysis of mosaic ontology for cloud resources annotation. In Computer Science and Information Systems (FedCSIS), 2011 Federated Conference on (pp. 973-980). IEEE.

[7] Quinton, C., Romero, D., §§ & Duchien, L. (2016). SALOON: a platform for selecting and configuring cloud environments. Software: Practice and Experience, 46(1), 55-78.

[8] Ribeiro, F. M., da Rocha, T., Santos, J. C., §§ & Moreno, E. D. (2016). A model-driven solution for automatic software deployment in the cloud. In Information technology: new generations (pp. 591-601). Springer, Cham.

[9] Szyperski, C. (2003, May). Component technology: what, where, and how?. In Proceedings of the 25th international conference on Software engineering (pp. 684-693). IEEE Computer Society.

[10] Turnbull, J. (2014). The docker book. Lulu. com.

A Clustering algorithm for distributing certificates in OLSR protocol

Mohammed Amine BOUDOUAIA [#1], Adda ALI PACHA [#2], Pascal LORENZ [*3]

[#] University of Science and Technology of Oran (USTO), BP 1505 El M'Naouar, 31036 Oran, Algeria

[1] Email : Boudouaia.amine.22@outlook.com

[2] Email : a.alipacha@gmail.com

* University of Haute Alsace, 34 rue du Grillenbreit, 68008 Colmar, France

[3] Email : lorenz@ieee.org

***Abstract*— Mobile Ad hoc Networks (MANET) define a novel architecture of wireless networks, where pre-established infrastructures are not necessary to communicate. Their mobile nodes are mainly designed to cooperate in order to manage their communications. However, security can be a crucial issue due to the absence of the infrastructure, which is often considered as a defence layer against cyber-attacks. In this paper, an improved model to distribute certificates in MANETs is proposed. Our work is based on optimized link state routing protocol (OLSR), where a novel yet-simple mechanism for forming clusters is introduced. The primary results of the proposal tend to be promising in terms of efficiency compared to some state-of-the art algorithms.**

***Keywords*—** *MANET, Certificate authority, OLSR, MPR*

1- INTRODUCTION

Currently, wireless networks have shown a great success thanks to their high extensibility. They are straightforward to be established and are less expensive, in which nodes can be inter-connected without using material support.

Thanks to the recent technologies in wireless communication and the powerful portable computing units, researchers are paying their attention in order to provide accessible information to anyone, anywhere and at any time.

Ad Hoc Mobile Networks (MANETs) tend to enhance the mobility of all components of the environment. Unlike networks with infrastructure, where the exchange of information must necessarily pass through an access point, the MANET does not include the entity "fixed site". All sites in the network are mobile and communicate in a direct way using their wireless communication interfaces [1]

MANETs can be exploited in all the applications, where the deployment of a centralized architecture might be complicated. Indeed, their robustness, low cost and rapid deployment made them involved in a wide range of applications including: Rescue operations, educational purposes, military applications, etc. [2]

However, the dynamic architecture of MANETs makes them very vulnerable to different attacks. In the attempt to overcome this issue, several studies were conducted in order to increase the level of security in MANETs. Public key infrastructures and digital certificates are considered one of the most promising techniques used in this field. These strategies exhibit cryptographic operations such as encryption and digital signature. The Certification Authority (CA) can be seen as the main and trusted component in the certification process. These operations ensure confidentiality, authentication, integrity and non-repudiation in electronic transactions [3].

Several approaches has been implemented to establish certificate distribution architectures in ad hoc networks. Indeed, a trivial approach is to centralize all the tasks of the CA in a single node [4]. However, this approach suffers from many problems. As a possible scenario, the main CA can be disabled for a given reason, which will result a heavy regeneration of new certificates for all the network components.
Furthermore, the dynamic nature of MANETs and lack of infrastructure make the implementation of PKI architecture and key of management very difficult. Recently, various research communities are leading projects in the attempt of implementing PKI infrastructures in MANETs. Following this context, an improved mechanism based on a routing protocol called OLSR (optimized link state routing protocol) is proposed in the aim of obtaining a competitive performance.

The rest of the paper is structured as follows. In the next section, an overview of the OLSR protocol is described. In Section 3, we will present a description of the distributed certificate authority (DCA) and its use in Ad-hoc networks. The proposed cluster creation algorithm is presented in section 4. Finally, the paper is concluded giving some perspectives.

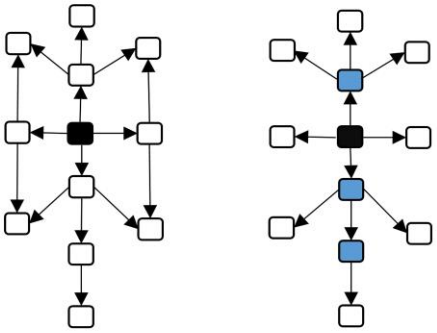
2- THE OLSR PROTOCOL

The Optimized link state Routing Protocol is a routing protocol proposed by the HIPERCOM-INRIA project team. It is defined in RFC 3626. OLSR is considered as one of the most important routing protocols for MANETs [5].

Unlike reactive routing protocols that create routes on demand (for example Ad-hoc On-demand Distance Vector), in OLSR, routing tables are initially established, which will provide available routes permanently. These routes are chosen based on hop count as a metric [1]

OLSR is a class of LSR (link state routing). In LSR, all nodes have the same priority. Each node declares these links and retransmits the message it receives which causes a great overload in the network. The goal of OLSR is to implement an optimized mechanism in order to avoid this overload. The main idea used in OLSR is to exploit multipoint relays (MPRs)

The reason behind the concept of multipoint relays is to reduce superfluous retransmissions of messages. The general idea of MPRs is to choose a group of nodes (one or more) of the first level to forward information to all the nodes of the second level. These nodes are considered MPR nodes. This mechanism optimizes the propagation in the networks and avoids the retransmission of control messages, which would save the bandwidth as it can be seen in Figure 1. [1, 5]



(a) (b)

Figure 1: (a) pure flood (b) with the MPR technique

Thereby, the OLSR protocol has two main features:

- Neighbours detection is ensured thanks to the periodic sending of HELLO messages and the election of multipoint relays.
- The topology management is ensured through the set of messages (topology control, multiple interface declaration and host and network association) that provide a global view of the topology for each node in the network.

In OLSR, these messages are periodically sent. The descriptions for each message are briefly described as follows [5]:

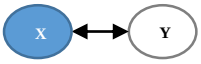
- **HELLO message:** Periodically, each node sends this message to its one hop neighbours. it contains information about the neighbours, the type of link (symmetric or asymmetric) and the intention of the node to become MPR.
- **Topology de control (TC):** sent to all nodes of the network to build the routing table. This message can be only sent by MPR node. It contains the set of neighbors who have chosen this node as a MPR.
- **Multiple interface declaration (MID), Host and network association (HNA):** announced by nodes that have multiple interfaces. The MID provides the ability to control the multiple use of interfaces, and the HNA provides the ability to connect a MANETs network with a wired network.

2.1- MPR selection:

- *Let $f(x)$ the neighborhood of node x:*

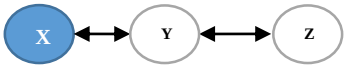
We suppose that:

$$If \quad y \in f(x)$$
$$And \quad x \in f(y)$$



$$Then \ \boldsymbol{the\ link\ is\ symmetric}$$

- $f_2(x)$ ⟶ the second neighbourhood of the node



$$F_2(x) = \{Z \notin f(x) / \exists\, g \in f(x) \text{ and } z \in f(y)\}$$
$$For\ y \in f(x) we\ define:$$
$$F_2(x,y)\{z \notin f(x) \text{ and } z \in f(y)\} f(x)$$
$$\mid F_2(x) = \bigcup_{Y \in f(x)} F_2(x,y)$$

2.2- The selection algorithm:

In this section, we present a brief description of the algorithm *Simple Greedy MPR Heuristic* [6], where two stages are defined:

- the first is the selection of the nodes of 1-hops $y \in f(x)$

Which covers the isolated nodes:

$$Y \in f(x)\ \exists\, \boldsymbol{z} \in f_2(x,y), |f(z) \cap f_2(x)| = 1$$
$$\rightarrow y \in MPR(x).$$

- Among the remaining nodes of the 1-hops f (x), the node x must choose the ones covering the largest $f_2(x)$ which have not been yet covered.

3- CERTIFICATE AUTHORITY IN MANETS:

The lack of infrastructure, auto configuration and high mobility makes ad hoc networks often used in different fields. However, despite these advantages, these networks can be vulnerable and fragile to a wide range of security attacks (passive and active). To deal with these security issues, researchers are proposing different approaches to increase the level of security in MANETs. Most of these proposals are based on public key cryptography that assures: privacy, integrity, authentication and other security services.

Certificates are among the main structures that rely on the PKI architecture. The CA are trusted third parts that authenticate entities (user certificate management) and secure communications in a given network. It also allows the revocation, the update and the renewal of certificates.

The aforementioned characteristics of the ad hoc networks complicates the adoption of a certificate management. For this reason, several research projects have been conducted to solve these problems by proposing several approaches. In the literature, two main solutions are generally applied:

- The first solution is to create a web of trust-based schemes (WOT), where each node of the network can validate the certificates of the other members. The major problem of this proposal is the high risk of having malicious node validating certificates. If this node is a member of the network, it can easily generate and validate false certificates to its neighbours [7].
- The second solution is to centralize all CA tasks in a single entity, where two structures are used: dependent CA that can be used in ad hoc networks with infrastructure, and independent CA that can be used in MANETS and are called Distributed Certificate Authority (DCA) .[4]

The general concept of DCA mechanism is to share the private key of the DCA node with a number of DCA shareholder nodes. The signatures of the certificates issued by the DCA can be verified by all nodes of the network with the public key which must be known by all the entities of the network.

The Distributed Certificate Authority scheme can be classified into two models:

(a) **Fully distributed certificate authority (FDCA):** This mechanism can improve the network performance in terms of availability and reduction of communication times. Its principle is the consideration of each node in the network as CA. Subsequently, it can generate partial certificates to the other nodes [8].

(b) Partially distributed certificate authority (PDCA): The selected nodes in the network (in terms of energy, the number of links or even clusters heads in networks that are based on clusters.etc...) will perform all the functionalities of the CA and can subsequently generate partial certificates [9]**.**

3.1- Related Work:

Zhou and al [9] have proposed a mechanism that shares the tasks of Certificate authority on a set of nodes, (k, n) threshold cryptography is used. In this study, it has been assumed that each entity in the network has a pair of keys (public / private) as it can be seen in Figure 2. First, the public key should be known by all the nodes of the network. Thereafter, the private key is shared between a set of servers, where each server acts as CA and generates a partial certificate. All of these certificates are collected by a node (C combiner) to calculate a valid certificate and then send it to the client. The authors have also proposed to select a subset of DCA nodes as a combiner to prevent the malicious nodes from accessing the network, and acting as a combiner.

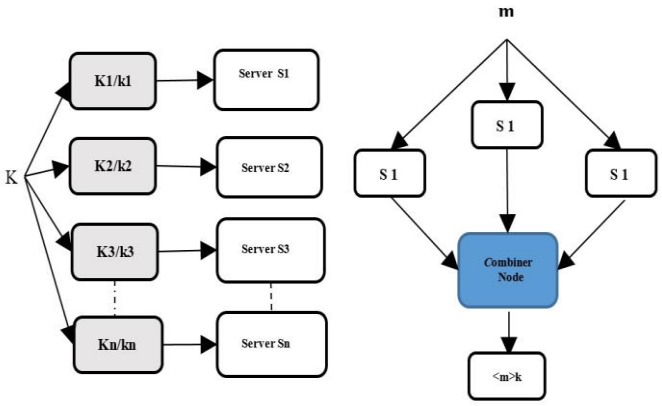


Figure 2: threshold cryptography configuration

Takehan and al [10] have proposed a certificate management approach in OLSR protocol. The idea is to choose a certificate management node (CMN) that manages the certificates based on the behaviour of other nodes in the network. To become a CMN, they take the parameters of willingness that are used when selecting MPRs. However, these parameters are not enough because a malicious node can easily falsify its willingness by setting a raised value. Therefore, the network will have a high security vulnerability. To prevent this issue, the authors enhanced their work with a voting method to add a value to the selection of CMNs. The author did not consider the revocation certificates. Moreover, they did not take into account the mobile nature of the networks, where the nodes can leave the reach of the CMNs.

R. Mehra and al [11] have proposed a clustering approach for VANETs. The proposed algorithm is based on the OLSR routing protocol. The main goal of this work is to optimize the protocol performance using clustering. Clusters will be formed based on certain parameters such as the confidence value and the position of the nodes.

M. Massari and al [12] presented a study of several approaches to adopt the certificate management system in ad hoc networks, and made an analysis of the advantages and disadvantages of each proposed solution. The author also included a comparative study on the overheads caused by validation and rescission operations. They also proposed the features of the ideal DCA system for MANETs.

R.Sugumar and al [13] have proposed a trust-based authentication scheme for cluster-based VANETs. The latter will be formed with respect to the degree estimation of confidence. The nodes with highest degree will act as cluster heads. The purpose of this work is to detect malicious nodes. The author has developed a system, where communications will be signed only by the sender and encrypted by a public/private key as distributed by a trusted authority and decrypted by the destination.

M. Ashwin and al [14] presented a study on the classification algorithm based on trust in MANETs. The authors proposed in the first part of the work an algorithm to form clusters to perform the election of the clusters heads CH. The algorithm is based on the energy and the mobility of the node (the node which has a low mobility to be elected as a cluster head). In the second part, the authors proposed a trust model weighted clustering algorithm.

S.Boukli-Hacene and al [15] proposed an improvement of the certificate distribution system for the CBRP (cluster based routing protocol) proposed by Hahn et al [16]. The proposal has been equipped with pre-emptive predictor to minimize the cost of generating and renewing certificates when moving nodes in the network. The idea of this work is that if one node in a given cluster are migrating to another cluster, then the cluster-head predict this intention and subsequently send its certificate to the other cluster-head through gateway nodes.

4- OUR PROPOSAL:

In certificate management mechanisms, the certificate authority generates certificates for clients to identify them and to provide secure communications. The problem in ad hoc networks, and more precisely the OLSR routing protocol increases because of these features (mobility, Auto-configuration and lack of infrastructure). For instance, in the case where a certification authority generates a certificate for a client, this latter will update it. The client will be obliged to contact the CA that has generated this certificate.

Moreover, since the environment is mobile, the node risks leaving the original CA. A request for a new certificate will be required, which will cause an overload of certificates in the network. Our works is to minimize this overload with the least cost of communication. The proposal uses the chaining mechanisms of certificates and clusters while exploiting the routing parameters of the OLSR protocol. Two main sections are presented:

1- In the first part, a mechanism to form clusters and choose the cluster-heads in the OLSR protocol is proposed.

2- In the second part, a solution to improve key management in the OLSR protocol is introduced.

4.1- The mechanism for creating clusters:

The clusters will be formed at the base of the *HELLO messages* that are periodically sent by each node of the network. The field <*Link Code*> is used to choose the nodes that will be elected as Heads clusters. The idea is to select the MPR nodes that have more symmetric links with the other MPRs. These nodes are considered as cluster heads and the two-hop neighbouring nodes are considered as cluster members. Therefore, our topology will be virtually divided into multiple clusters.

4.2 The cluster formation algorithm:

Before performing the proposal, a web of trust should be established, which follows a representation of our procedure. It should be stated that our algorithm takes place only after the creation of the clusters.

MPR_ONE	MPR node that has links with isolated nodes
MPR_TWO	MPR node that has links to MPR_ONE nodes
VAL_NODE_FINAL	value reset to 1, assigned to each end node
VAL_MPR_ONE	it is a value calculated by each node MPR ONE and is equal to the SUM of the received VAL_NODE_FINAL
VAL_LINK	number of MPR links of each TWO MPR

Table 1 Notation description

The notations that will be used in the following steps are defined in Table 1.

The algorithm can be described as follows:
Step 1: each end node sends the value "VAL_NOD_FINAL" to its MPR (the value is initialized to 1).

Step 2: the node MPR_ONE, will have a value VAL_MPR_ONE (sum VAL-NOD-FINAL).

Step 3: each MPR_ONE sends the value (VAL_MPR_ONE + 10) to its neighbour MPR_TWO. If it has several MPR_TWO, then it chooses MPR_TWO which has a higher value Val_LINK. The node MPR_TWO will be a cluster Head. The node MPR_ONE and the end nodes will be cluster members.

Step 4: the nodes that have one or two hops neighbouring with a cluster head will be assigned directly to that cluster. If the node with two or more cluster head neighbours are at the same level, it chooses the cluster head which has the largest cluster members value.

Step 5: we put in the set N all the nodes that are assigned to a cluster (cluster heads and cluster members).

Step 6: we delete the N (we suppose that all the nodes are assigned to clusters).
Step 7: we repeat the steps until we cover all the nodes in the networks. Figure 3 sums up the process of our proposal.

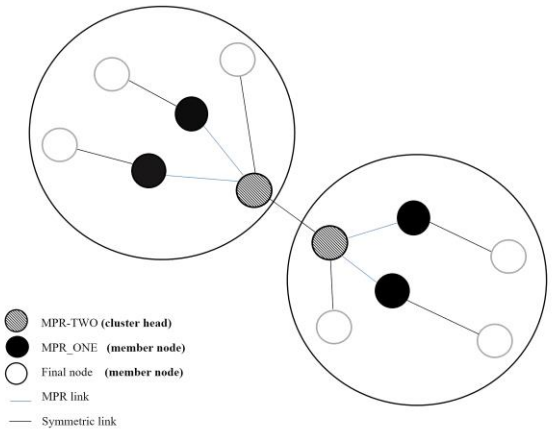


Figure 3: creating clusters

4.3- Certificates chaining:

Our proposal aims to authenticate the nodes in the network by using the certificate chaining. The creation of clusters using our algorithm would allow the creation of an appropriate environment to exploit the chaining principle of certificates. The solution assumes that each node in the network generates a key pair (decentralized generation) and sends a signature request (CSR: certificate request signing) to its cluster-head (MPR_TWO). The cluster-head will act as a certificate authority in order to generate a new certificate.
The MPR_ONE node is supposed to be the Registration Authority (RA). It will be an intermediate entity between the clients (endpoints) and the certification authority (cluster-head) as it can be noticed in Figure 4.

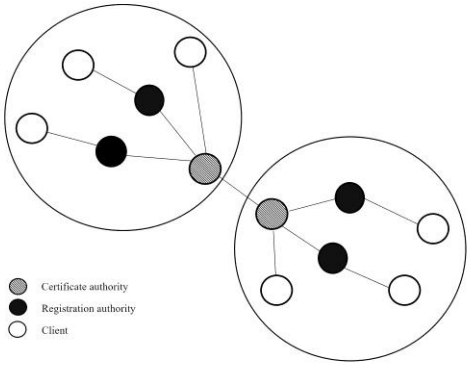


Figure 4: Architecture of Public Key Infrastructure

The following figure shows the process of obtaining a certificate:

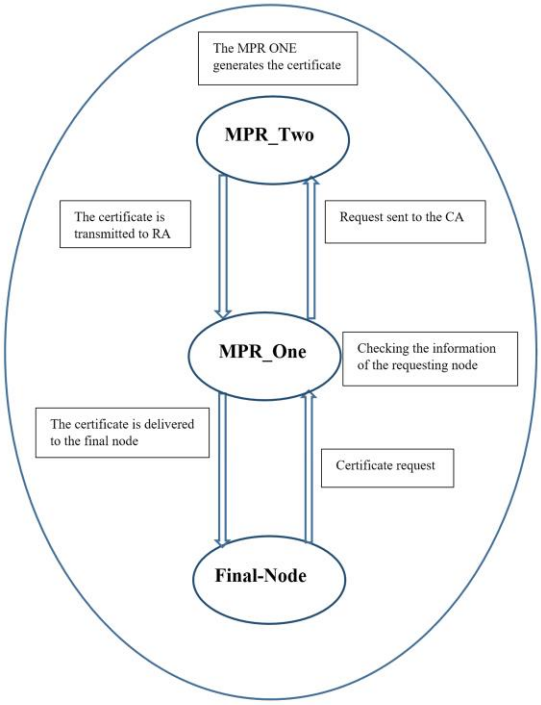


Figure 5: The certificate obtaining process

After the clustering process, each member node requests a certificate from its cluster-head. If the node changes cluster (cause of mobility), then his certificate will be expired and he requests a new certificate from his new cluster-head. Furthermore, each certificate has a validity period. The member node will be able to request a renewal as soon as its certificate expires. Several changes may revoke a certificate (a change of information, loss of private keys ... etc). For this reason, the mechanism requires a CRL table (certificate revocation list) to store all revoked certificates. Each entry of the table contains the node MAC address along with the number of its certificate.

5- Conclusion:

This study presents different solutions to secure MANET's networks. The goal of our solution is to create clusters in the OLSR protocol. The main idea is to choose the MPR node that has the most MPR links compared to the neighbouring nodes to choose it as a cluster-head. Thereafter, we proposed a solution to distribute certificates based on our cluster creation algorithm. In the near future, we aim to implement this proposal and evaluate its effectiveness. We also aim to propose a new strategy to minimize the generation of certificates in the case where nodes are moved from one cluster to another.

References:

[1] Kamel Saddiki , Sofiane Boukli-Hacene , Pascal Lorenz , Marc Gilg "Black hole attack detection and ignoring

in OLSR protocol" International Journal of Trust Management in Computing and Communications , Vol. 4 , 2017.

[2] Rachna Jain , Indu Kashayap " Survey Of Energy Award Link Stable Routing Protocols In MANETs" 2nd International Conference On Trends In Electronics And Information (ICOEI), 2018.

[3] Ruo Jun Cai , Xue Jun Li, and Peter Han Joo Chong "An Evolutionary Self-Cooperative Trust Scheme Against Routing Disruptions in MANETs" IEEE Transactions on Mobile Computing , PP. 42 – 55 , 2018.

[4] L. Zhou, F. B. Schneider, and R. V. Renesse, "COCA: A secure distributed online certification authority," Journal ACM Transactions on Computer Systems (TOCS), Vol. 20, pp. 329-368, 2002.

[5] Clausen .T and Jacquet .P, "RFC 3626 - Optimized Link State Routing Protocol (OLSR)," 2003.

[6] Anthony Busson, Nathalie Mitton, Eric Fleury. An analysis of the MPR selection in OLSR and consequences. Mediterranean Ad Hoc Networking Workshop (MedHocNet'05), Jun 2005.

[7] J.-P. Hubaux, L. Butty, and S. Capkun, "The quest for security in mobile ad hoc networks," In Proceedings of the the 2nd ACM international symposium on Mobile ad hoc networking & computing, Long Beach, CA, USA, pp. 146-155, 2001.

[8] D. Joshi, K. Namuduri, and R. Pendse, "Secure, redundant, and fully distributed key management scheme for mobile ad hoc networks: an analysis," EURASIP Journal of Wireless Commununication Network, Vol. 2005, pp. 579-589, 2005.

[9] L. D. Zhou and J. Z. Hass "Securing ad hoc networks," Ieee Network, vol. 13, pp. 24-30, 1999.

[10] Y. Takehana, I.Nishimura, N. Yosaka, T. Nagase, and Y. Yoshioka "Building Trust among Certificate Management Nodes in Mobile Ad-Hoc Network", 26th International Conference on Advanced Information Networking and Applications Workshops, 2012.

[11] ruchi mehra , rasmeet s. bali , prabhsharan kaur " efficient clustering based olsr routing protocol for VANET " symposium on colossal data analysis and networking (CDAN) , 2016.

[12] M. Masdari , J.P.Barbin "Distributed Certificate Management in Mobile Ad Hoc Networks", International Journal of Applied Information Systems (IJAIS),VOL.4 , 2012.

[13] R.Sugumar , A.Rengarajan , C.Jayakumar "Trust Based Authentication Technique For cluster Based Vehicular Ad-hoc Networks (VANET)", Wireless Networks , Vol. 24, pp.373-382 , 2018.

[14] M.Ashwin , S.Kamalraj , M.Azath "Weighted Clustering Trust Model For Mobile Ad hoc Networks" , Vol.94 , pp.2203-2212 , 2017.

[15] Boukli-Hacene Sofiane , Ouali abdelkader , Bassou Asmaa "Predictive Preemptive Certificate Transfer in Cluster-Based Certificate Chain" , International Journal of Communication Networks and Information Security (IJCNIS) , Vol. 6, PP.44-51, 2014.

[16] G. Hahn, T. Kwon, S. Kim, and J. Song, "Cluster-Based Certificate Chain for Mobile Ad Hoc Networks," in International Conference on Computational Science and Its Applications (ICCSA), pp. 769-778, 2006.

Double Skew $(1+u)-$Constacyclic Codes over $\mathbb{Z}_4(\mathbb{Z}_4+u\mathbb{Z}_4)$

1st Ahlem Melakhessou
Faculty of Mathematics and Informatics
Department of Mathematics, Mostefa Ben Boulaïd University
Batna, Algeria
a.melakhessou@univ-batna2.dz

2nd Kenza Guenda
Faculty of Mathematics
University of Science and Technology Houari Boumedien
Algiers, Algeria
ken.guenda@gmail.com

***Abstract*—In this document, we study skew constacyclic codes over the ring $\mathbb{Z}_4R$ where $R=\mathbb{Z}_4+u\mathbb{Z}_4$, for $u^2=0$. We give the definition of these codes as subsets of the ring $\mathbb{Z}_4^{\alpha}R^{\beta}$. Further, we have generalized these codes to double skew $(1+u)-$constacyclic codes over $\mathbb{Z}_4R$.**

***Index Terms*—codes over ring, skew cyclic, constacyclic, skew constacyclic, double skew constacyclic.**

I. Introduction

One of the most important problems in coding theory is to construct codes with as large a minimum Hamming distance as possible. Many algebraic methods have been employed to achieve this goal. Cyclic codes and their various generalizations such as constacyclic codes and quasi-cyclic (QC) codes have played a key role in this quest. Yet another generalization of cyclic codes, called skew cyclic codes, was introduced in [**?**] which have been the subject of an increasing research activity over the past decade. On the other hand, codes over rings received much attention in the past few decades. Consequently, algebraic structures of cyclic, skew cyclic, and constacyclic codes over various rings are determined ([**?**], [**?**], [**?**], [**?**]). Recently, P. Li et al. [**?**] gave the structure of $(1+u)$-constacyclic codes over the ring $\mathbb{Z}_2\mathbb{Z}_2[u]$ and Aydogdu et al. [**?**] studied $\mathbb{Z}_2\mathbb{Z}_2[u]$-cyclic and constacyclic codes. Further, Jitman et al. [**?**] considered the structure of skew constacyclic over finite chain rings. The work is organized as follows. We first give some basic results about the ring $R=\mathbb{Z}_4+u\mathbb{Z}_4$, where $u^2=0$, and linear codes over $\mathbb{Z}_4R$. In Section 5, we study the algebraic structure of skew constacyclic codes over the ring $\mathbb{Z}_4R$. A necessary and sufficient condition for a skew constacyclic code over $\mathbb{Z}_4R$ to contain its dual is given. These codes are then further generalized to double skew $(1+u)-$constacyclic codes.

II. Preliminaries

Let (α,β) denote $n=\alpha+2\beta$ where α and β are positive integers. Consider the ring $R=\mathbb{Z}_4+u\mathbb{Z}_4$, where $u^2=0$. The ring R is isomorphic to the quotient ring $\mathbb{Z}_4[u]/\langle u^2\rangle$. The units of R are

$$1,3,1+u,1+2u,1+3u,3+u,3+2u,3+3u,$$

and the non-units are

$$0,2,u,2u,2+u,2+2u,3u,2+3u.$$

The ring R is not a chain ring, whereas it is a local ring with the maximal ideal $\langle 2,u\rangle$. Each element r of R can be expressed uniquely as

$$r=a+ub,\ \text{where } a,b\in\mathbb{Z}_4.$$

An element $a+ub$ of R is a unit if and only if a is unit. For a linear code C_β of length β over R, its torsion $Tor(C_\beta)$ and residue $Res(C_\beta)$ codes are codes over $\mathbb{Z}_4$, defined as follows

$$Tor(C_\beta)=\{b\in\mathbb{Z}_4^{\beta}:\ ub\in C_\beta\}$$

and

$$Res(C_\beta)=\{a\in\mathbb{Z}_4^{\beta}:\ a+ub\in C_\beta \text{ for some } b\in\mathbb{Z}_4^{\beta}\}.$$

Next we construct the ring

$$\mathbb{Z}_4R=\{(e,r):\ e\in\mathbb{Z}_4, r\in R\}.$$

The ring $\mathbb{Z}_4R$ is not an R-module under the operation of standard multiplication. To make $\mathbb{Z}_4R$ an R-module, we follow the approach and define the map

$$\eta: R\to\mathbb{Z}_4$$
$$a+ub\mapsto a.$$

Then, for any $d\in R$, we define the multiplication $\star$ by

$$d\star(e,r)=(\eta(d)e,dr).$$

This multiplication can be naturally generalized to the ring $\mathbb{Z}_4^\alpha R^\beta$ as follows.
For any $d \in R$ and $v = (e_0, e_1, \ldots, e_{\alpha-1}, r_0, r_1, \ldots, r_{\beta-1}) \in \mathbb{Z}_4^\alpha R^\beta$ define

$$dv = (\eta(d)e_0, \eta(d)e_1, \ldots, \eta(d)e_{\alpha-1}, dr_0, dr_1, \ldots, dr_{\beta-1}),$$

where $(e_0, e_1, \ldots, e_{\alpha-1}) \in \mathbb{Z}_q^\alpha$ and $(r_0, r_1, \ldots, r_{\beta-1}) \in R^\beta$. Let C be a $\mathbb{Z}_4R$-linear code and let C_α (respectively C_β) be the canonical projection of C on the first α (respectively on the last β) coordinates. Since the canonical projection is a linear map, C_α and C_β are linear codes over $\mathbb{Z}_q$ and over R of length α and β, respectively. A code C is called separable if C is the direct product of C_α and C_β, i.e.,

$$C = C_\alpha \times C_\beta.$$

A. Skew Polynomial Ring $R[x;\theta]$

The structure of the non-commutative ring $R[x;\theta]$ depends on the elements of the commutative ring R and an automorphism θ of R. Note that an automorphism θ of R must fix every element of $\mathbb{Z}_q$, hence it satisfies $\theta(a+ub) = a+\theta(u)b$. Therefore, it is determined by its action on u. Let $\theta(u) = 2 + 2u$. Then, $\theta(a + ub) = a + \theta(u)b = a + (2 + u)b$ for all $a + ub \in R$. Let θ be an automorphism of R and let m be its order. The skew polynomial ring $R[x;\theta]$ is the set of polynomials over R where the addition of these polynomials is defined in the usual way while multiplication $*$ is defined using the distributive law and the rule

$$x * a = \theta(a)x.$$

The set $R[x;\theta]$ with respect to addition and multiplication defined above form a non-commutative ring called the skew polynomial ring. An element $g(x) \in R[x;\theta]$ is said to be a right divisor (resp. left divisor) of $f(x)$ if there exists $q(x) \in R[x;\theta]$ such that

$$f(x) = q(x) * g(x) \quad (\text{ resp. } f(x) = g(x) * q(x)).$$

In this case, $f(x)$ is called a left multiple (resp. right multiple) of $g(x)$.

Lemma 2.1: [**?**, Lemma 1] Let $f(x)$, $g(x) \in R[x;\theta]$ be such that the leading coefficient of $g(x)$ is a unit. Then there exist $q(x)$, $r(x) \in R[x;\theta]$ such that

$$f(x) = q(x) * g(x) + r(x),$$

where $r(x) = 0$ or $\deg(r(x)) < \deg(g(x))$.

III. $\mathbb{Z}_4R$ -Linear Skew $(1+u)-$Constacyclic Codes

In this section, we study skew $(1 + u)$-constacyclic codes over the ring $\mathbb{Z}_4R$.

Definition 3.1: Let θ be an automorphism of R. A linear code C over $\mathbb{Z}_4^\alpha R^\beta$ is called skew constacyclic if C satisfies the following two conditions.

(i) C is an R-submodule of $\mathbb{Z}_4^\alpha R^\beta$,

(ii)

$$(e_{\alpha-1}, e_0, \ldots, e_{\alpha-2}, (1+u)\theta(r_{\beta-1}), \theta(r_0), \ldots, \theta(r_{\beta-2})) \in C.$$

whenever

$$(e_0, e_1, \ldots, e_{\alpha-1}, r_0, r_1, \ldots, r_{\beta-1}) \in C$$

In polynomial representation, each codeword $c = (e_0, e_1, \ldots, e_{\alpha-1}, r_0, r_1, \ldots, r_{\beta-1})$ of a skew constacyclic code can be represented by a pair of polynomials

$$\begin{aligned} c(x) &= \left(e_0 + e_1x + \ldots + e_{\alpha-1}x^{\alpha-1}, r_0 + r_1x + \ldots + r_{\beta-1}x^{\beta-1}\right) \\ &= (e(x), r(x)) \in \mathbb{Z}_4[x]/\langle x^\alpha - 1\rangle \times R[x;\theta]/\langle x^\beta - (1+u)\rangle. \end{aligned}$$

Let $h(x) = h_0 + h_1x + \ldots + h_tx^t \in R\ [x;\theta]$ and let $(f(x), g(x)) \in \mathbb{Z}_4[x]/\langle x^\alpha - 1\rangle \times R[x;\theta]/\langle x^\beta - (1+u)\rangle$. The multiplication is defined by the basic rule

$$h(x)(f(x), g(x)) = (\eta(h(x))f(x), h(x) * g(x)),$$

where $\eta(h(x)) = \eta(h_0) + \eta(h_1)x + \ldots + \eta(h_t)x^t$.

Lemma 3.2: A code C of length (α, β) over $\mathbb{Z}_4R$ is a skew $(1 + u)$-constacyclic code if and only if C is left $R[x;\theta]$-submodule of $\mathbb{Z}_4[x]/\langle x^\alpha - 1\rangle \times R[x;\theta]/\langle x^\beta - (1+u)\rangle$.

Theorem 3.3: Let C be a linear code over $\mathbb{Z}_4R$ of length (α, β), and let $C = C_\alpha \times C_\beta$, where C_α is linear code over $\mathbb{Z}_4$ of length α and C_β is linear code over R of length β. Then C is a skew $(1 + u)$-constacyclic code with respect to the automorphism θ if and only if C_α is a cyclic code over $\mathbb{Z}_4$ and C_β is a skew $(1 + u)$-constacyclic code over R with respect to the automorphism θ.

Corollary 3.4: Let C be a linear code over $\mathbb{Z}_4R$ of length (α, β), and let $C = C_\alpha \times C_\beta$, where C_α is a linear code over $\mathbb{Z}_4$ of length α and C_β is a linear code over R of length β. Then C is a skew cyclic code with respect to the automorphism θ if and only if C_α is a cyclic code over $\mathbb{Z}_4$ and C_β is a skew cyclic code over R with respect to the automorphism θ.

IV. Double Skew Constacyclic Codes over $\mathbb{Z}_4R$

In this subsection, we study double skew constacyclic codes over $\mathbb{Z}_4R$. Let $n_1 = \alpha + 2\beta$ and $n_2 = \alpha' + 2\beta'$ be integers such that $n = n_1 + n_2$. We consider a partition of the set of

the n coordinates into two subsets of n_1 and n_2 coordinates, respectively, so that C is a subset of $\mathbb{Z}_4^{\alpha} R^{\beta} \times \mathbb{Z}_4^{\alpha'} R^{\beta'}$.

Definition 4.1: A linear code C of length n over $\mathbb{Z}_4 R$ is called a double skew constacyclic code if C satisfies the following conditions.

(i) C is a linear code.

(ii) If

$$\begin{pmatrix} e_0, e_1, \ldots, e_{\alpha-1}, r_0, r_1, \ldots, r_{\beta-1}, \\ e'_0, e'_1, \ldots, e'_{\alpha'-1}, r'_0, r'_1, \ldots, r'_{\beta'-1} \end{pmatrix} \in C$$

then

$$\begin{pmatrix} e_{\alpha-1}, e_0, \ldots, e_{\alpha-2}, (1+u)\theta(r_{\beta-1}), \ldots, \theta(r_{\beta-2}), \\ e'_{\alpha'-1}, e'_0, \ldots, e'_{\alpha'-2}, (1+u)\theta(r'_{\beta'-1}), \ldots, \theta(r'_{\beta'-2}), \end{pmatrix} \in C$$

Denote by $\mathfrak{R}_{\alpha,\beta,\alpha',\beta'}$ the ring $\mathbb{Z}_q[x]/\langle x^{\alpha}-1\rangle \times R[x;\theta]/\langle x^{\beta} - (1+u)\rangle \times \mathbb{Z}_q[x]/\langle x^{\alpha'} - 1\rangle \times R[x;\theta]/\langle x^{\beta'} - (1+u)\rangle$.
In polynomial representation, each codeword

$$c = \begin{pmatrix} e_0, e_1, \ldots, e_{\alpha-1}, r_0, r_1, \ldots, r_{\beta-1}, \\ e'_0, e_1, \ldots, e'_{\alpha'-1}, r'_0, r'_1, \ldots, r'_{\beta'-1} \end{pmatrix}$$

of a skew constacyclic code can be represented by four polynomials

$$\begin{aligned} c(x) &= \begin{pmatrix} e_0 + e_1 x + \ldots + e_{\alpha-1}x^{\alpha-1}, \\ r_0 + r_1 x + \ldots + r_{\beta-1}x^{\beta-1}, \\ e'_0 + e'_1 x + \ldots + e'_{\alpha'-1}x^{\alpha'-1}, \\ r'_0 + r'_1 x + \ldots + r'_{\beta'-1}x^{\beta'-1} \end{pmatrix} \\ &= (e(x), r(x), e'(x), r'(x)) \in \mathfrak{R}_{\alpha,\beta,\alpha',\beta'}. \end{aligned}$$

Let

$$h(x) = h_0 + h_1 x + \ldots + h_t x^t \in R\ [x;\theta]$$

and let

$$(f(x), g(x), f'(x), g'(x)) \in \mathfrak{R}_{\alpha,\beta,\alpha',\beta'}.$$

We define a multiplication by

$$h(x)(f(x), g(x)) = \begin{pmatrix} \eta(h(x))f(x), h(x) * g(x), \\ \eta(h(x))f'(x), h(x) * g'(x)), \end{pmatrix}$$

where $\eta(h(x)) = \eta(h_0) + \eta(h_1)x + \ldots + \eta(h_t)x^t$. This gives us the following Theorem.

Theorem 4.2: A linear code C is a double skew constacyclic code if and only if it is a left $R[x;\theta]$-submodule of $R_{\alpha,\beta,\alpha',\beta'}$.

CONCLUSION

In this paper double skew $(1+u)-$constacyclic codes are considered over the ring $\mathbb{Z}_4 R$, where $R = \mathbb{Z}_4 + u\mathbb{Z}_4$, $u^2 = 0$ and their algebraic and structural properties are studied.

REFERENCES

[1] I. Aydogdu, T. Abualrub and I. Siap, $\mathbb{Z}_2\mathbb{Z}_2[u]-$*cyclic and constacyclic codes*, IEEE Transactions on Information Theory, 63 (8) (2016), pp. 4883–4893.

[2] R. K. Bandi, M. Bhaintwal, *A note on cyclic codes over* $\mathbb{Z}_4 + u\mathbb{Z}_4$, Discrete Mathematics, Algorithms and Applications, 8 (1) (2016), pp. 1–17.

[3] D. Boucher, W. Geiselmann and F. Ulmer, *Skew-cyclic codes*, Appl. Algebra Engrg. Comm. Comput., 18(4)(2007), pp. 379–389.

[4] J. Gao, F. Ma and F. Fu, *Skew constacyclic codes over the ring* $\mathbb{F}_q + v\mathbb{F}_q$, Appl.Comput. Math., 6 (3) (2017), pp. 286–295.

[5] S. Jitman, S. Ling and P. Udomkavanich, *Skew constacyclic over finite chain rings*, Adv. Math. Commun., 6 (1) (2012), pp. 39–63.

[6] P. Li, W. Dai and X. Kai, *On* $\mathbb{Z}_2\mathbb{Z}_2[u] - (1+u)$*-additive constacyclic*, arXiv:1611.03169v1 [cs.IT] 10 Nov 2016.

[7] A. Sharma, M. Bhaintwal, *A class of skew-constacyclic codes over* $\mathbb{Z}_4 + u\mathbb{Z}_4$, Int. J. Information and Coding Theory, 4 (4)(2017), pp. 289–303.

Anonymous communication in IoT based on verifiable encryption

Khaled Hamouid
LaSTIC research laboratory
University of Batna 2
Batna, Algeria
k.hamouid@univ-batna2.dz

***Abstract*—This paper proposes a pseudonym-based authentication scheme for Internet of Things (IoT). The proposed scheme is intended to protect privacy of users and support anonymous communications in IoT. Based on the concept of verifiable encryption, our scheme allows to smart objects and users in the IoT to authenticate each other or prove that they have trustworthy relationship without revealing their identity attributes, thereby preserving their privacy and thwarting traffic analysis attacks. Through a security analysis, we demonstrate the reliability of our scheme.**

***Index Terms*—IoT, verifiable encryption, authentication, anonymity, privacy**

I. Introduction

Technological progress of wireless communication and smart devices has evolved quite spectacularly over the last decade, with the prospect of providing pervasive computing and ubiquitous environments whereby users may have access to information and services anywhere, anytime and from any mobile device. This evolution has led to the development of new network paradigms such as Wireless Sensor Networks, Vehicular Networks, Mobile Ad-hoc networks, etc.

The integration of these new paradigms and their foundations in the current Internet has given rise to the concept of IoT. In the near future, today's computer-based Internet is expected to evolve to an Internet of Things (IoT) where everything is connected [1], [2]. The vision of IoT is to provide a ubiquitous environment that integrates a wide range of heterogeneous objects with communication, computing and/or sensing capabilities such as : sensors, RFID tags, smart devices, etc [3]. There may also be everyday things like a vehicle, and appliance in the house, sensors in the road, etc. These objects interact with users and among themselves in seamless fashion to provide innovative and ubiquitous services. IoT is foreseen to improve our everyday lives by the provision of a wide range of services in various application domains such as smart cities, smart homes, eHealth, etc. [4]

In IoT, a large part consists of resource-constrained and vulnerable devices which communicate over wireless channel and may often be without protection. The growth in the number of such devices connected to IoT results in many security issues [5]. It is particularly challenging to protect the privacy of users against unauthorized tracking in IoT environment where identities of things are traceable and linkable to real owners, especially with current solutions such as RFID, NFC, etc.

Anonymous communication protocols seem to be a good solution to provide privacy preserving. The underlying idea is to hide the identity attributes of IoT communicating objects in order to prevent adversaries from identifying them and acquiring user-related private information by means of traffic analysis attacks.

However, how to achieve authentication along with anonymous communications is another major issue. Indeed, the goals of privacy and authentication are conflicting. On the one hand, in order to authenticate a communicating object, it is necessary to provide its identity. On the other hand, revealing the real identity attributes is not privacy-preserving. Traditional anonymity techniques in wireless networks are mainly focusing on unlinkable data delivery [6], but cannot ensure authentication. Furthermore, authentication protocols [7], [8] do not take into consideration anonymity.

In the literature, there are some attempts to tackle this issue. Data tagging for managing privacy [9] is proposed. However, according to [1], this approach generates an excessive overhead, which is not suitable for IoT. Other techniques such as pseudonym's certificate [10] are proposed to provide anonymous authentication. However, according to [11], this requires the IoT smart objects to hold a large number of pseudonyms and corresponding certificates. This imposes high overheads to smart objects with insufficient computing and storage resources.

Being motivated by above issues, we propose in this paper a pseudonym-based authentication scheme to protect privacy of communicating objects in IoT. Based on the concept of verifiable encryption [12], the proposed scheme meets three appealing features: 1) it offers conditional anonymity where objects communicate with pseudonyms instead of their real identities, 2) objects, even anonymous, still able to authenticate themselves and verify whether an object is an authorized participant in the system, 3) only a Trusted Authority (TA) can revoke anonymity of smart objects and reveal their real identity.

In the remainder of this paper, we first present the underlying cryptographic building blocks in section II. Then, we present our solution in detail in section III. The security of our scheme is analyzed in section IV. Finally, we conclude the paper in section V.

II. Preliminaries

A. Verifiable encryption

Verifiable encryption protocol is a "*zero knowledge*" protocol where a prover P proves to a verifier V that an encrypted message m satisfies a particular property, without revealing any useful information about m.

Camenisch *et al.* [12] proposed a verifiable encryption scheme for Discrete Logarithms (DL). Verifiability is achieved by a *zero-knowledge proof protocol (PoK)* to prove properties related to discrete logarithms. Camenisch's scheme consists of an encryption scheme and zero-knowledge proof protocol, which are briefly described in the following:

- **Public-key encryption algorithm:**
  - Key generation: Select two random primes p', q' and compute $p = 2p' + 1, q = 2q' + 1, N = pq$. Choose $g' \in \mathbb{Z}^*_{N^2}$ and compute $g = (g')^{2N} \ (mod\ N^2)$. Picks a random $x \in [N^2/4]$ as the secret key, and compute $y = g^x \ (mod\ N^2)$ as the corresponding public-key, where $[a]$ denotes the set $\{0, ..., \lfloor a - 1 \rfloor\}$, and $\lfloor a \rfloor$ is the largest integer $\leq a$.
  - Encryption: To encrypt $m \in [N]$ using the public-key y, picks a random $r \in [N/4]$ and compute $u = g^r \ (mod\ N^2), e = y^r h^m \ (mod\ N^2)$, wehere $h = 1 + N \ (mod\ N^2)$. Outputs the encryption of m: $c = (u, e)$.
  - Decryption: to decrypt a ciphertext $c = (u, e)$ using the secret key x, compute $\hat{m} = (e/u^x)^{2t} \ (mod\ N^2)$, where $t = 2^{-1} \ (mod\ N)$. The decryption is m if $\hat{m}$ is of the form h^m.
- **Zero-knowledge proof of a Discrete Logarithm (DL):** Assume a ciphertext c as an encryption of a message m under a given public-key y. Zero-knowledge proof of DL, denoted $PoK\{(m) : c = E_y(m) \wedge \delta = \gamma^m\}$, is a two-party protocol whereby the encryptor (prover) P of m proves to a verifier V that the ciphertext c is an encryption under y of $log_\gamma \delta$ (discrete logarithm of an element δ with respect to base γ), where c, δ, γ are publicly known. Fig.1 presents a simplified version of Camenisch's zero-knowledge proof of DL.

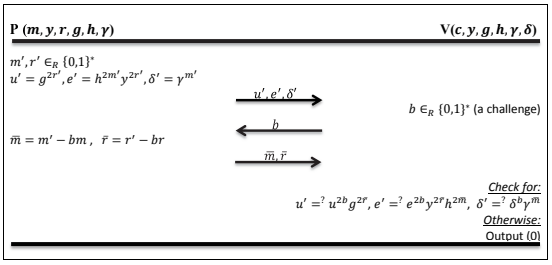


Fig. 1. Zero-knowledge proof (PoK) of a discrete logarithm

B. Schnorr signature

The Schnorr signature scheme [13] is a variation of discrete-log based signature schemes, which is similar to ElGamal and DSA (Digital Signature Algorithm). The security of Schnorr scheme, similarly to ElGamal and and DSA, is based on the intractability of *the Discrete Logarithm Problem* (DLP), which is, given a cyclic group G of order prime q with a generator g, given g^x for random $x \in \mathbb{Z}^*_q$, it is hard to find x. Schnorr signature scheme has been proven to be secure under the random oracle model. Schnorr signature scheme is described as follows:

- ***Setup:***
  - Choose large primes p and q with q factor of $p - 1$.
  - Choose a generator g in cyclic group G of prime order q.
  - Choose a one-way hash function $H : \{0, 1\}^* \longrightarrow \mathbb{Z}_q$
- ***Key generation:***
  - Choose a random number $sk \in \mathbb{Z}^*_q$ as the user's private-key.
  - Computes the corresponding public-key as: $pk = g^{sk} \ (mod\ p)$
- ***Sign*** (sk, m):
  - Selects a random number $k \in Z^*_q$
  - Calculates $r = g^k \ (mod\ p)$ and $s = sk.H(m||r) + k \ (mod\ q)$, where m is the message to sign.
  - Outputs the signature $\sigma = (r, s)$.
- ***Verify*** (pk, m, σ):
  - If $g^s \ =^? \ pk^{H(m||r)}.r$, output *Valid*, else output *Invalid*.

III. The proposed anonymous communication scheme

A. System model

In our model, each communicating IoT node i has an identity attributes (ID_i) to which is associated a pseudonym (PS_i). The IoT nodes communicate anonymously by using the associated pseudonyms rather than real identities. Authentication is implicitly provided from the pseudonyms and without the need of certificates.

We assume a Trusted Authority (TA) which is responsible for managing the anonymity and the revocation of IoT members. More precisely, the TA has the following tasks: 1) generating and distributing the verifiable pseudonyms for IoT members, 2) providing traceability and revocation of misbehaving IoT anonymous members. To achieve these tasks, the TA uses three private/public keys pairs $\{(x_1, Y_1), (x_2, Y_2), (a, A)\}$, where $x_1, x_2, a \in_R \mathbb{Z}_q$ (for prime q), $Y_i = g_i^{x_i} \ (i = 1, 2)$, $A = g_2^a$, and g_1, g_2, g are generators of cyclic groups G_1, G_2, G respectively.

It is important to note that the TA takes action only in the registration (pseudonym distributing) phase and when a revocation of anonymity is required. This means that IoT nodes can communicate anonymously while ensuring mutual authentication without involving the TA. The figure 2 illustrates our anonymous communication model.

The pseudonyms as generated by our scheme satisfy the following properties :

- *Verifiability*: The authenticity of pseudonyms could be verified implicitly by any IoT node without involving the TA. Invalid pseudonyms can be easily detected.
- *Unforgeability*: No one other than the TA can forge a verifiable pseudonym. A valid pseudonym can only be issued by the TA based on the real identity of the pseudonym holder.
- *Unlikability*: Pseudonyms do not provide any useful information about real user's identities.
- *Traceability*: In pseudonyms may be revoked only by the TA in order to trace back misbehaving nodes. Given a pseudonym PS_i, the corresponding identity ID_i can be extracted only by the TA. Traceability is used to detect and revoke misbehaving anonymous nodes.

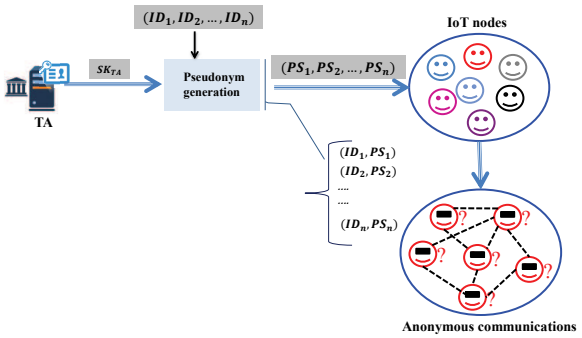


Fig. 2. Proposed anonymous communications model

B. Pseudonym's generation protocol

To satisfy the pseudonym properties defined previously, we propose a pseudonym generation protocol based on Camenisch's verifiable encryption scheme [12]. Roughly speaking, a pseudonym is generated as a composite of two cryptographic functions. First, the real identity (ID_i) of node i is signed by the TA's secret-key x_2 based on Schnorr's scheme [13]. This produces a signature denoted PS'_i. The latter is then encrypted by the TA's public-key (Y_1) based on the verifiable encryption algorithm. This results in a verifiable pseudonym PS_i.

Given the TA's credentials $\{x_2, a, Y_1, A\}$ and the setup parameters $(g_1, g_2, H(.))$, the pseudonym generation protocol for a given IoT node i is as follows:

- **Registration**
  - i generates a random secret $r_i \in \mathbb{Z}_q$, and computes $u_i = g_1^{r_i}$.
  - i transmits a pseudonym request, that includes its identity (ID_i) as well as the pseudonym's verification public parameters $(u_i, Y_1^{r_i})$, to the TA.
  - The TA verifies the validity of public parameter u_i as:
$$u_i^{x_1} =^{?} Y_1^{r_i} \quad (1)$$
- **Identity signature**
  - The TA computes the following signature on ID_i:
$$PS'_i = x_2.H(ID_i||A) + a \quad (2)$$
- **Verifiable Encryption of identity signature (PS'_i)**
  - The TA produces the verifiable pseudonym of node i as an encryption of PS'_i using the TA's public-key Y_1:
$$PS_i = enc(PS'_i)_{Y_1} = g_2^{PS'_i}.u_i^{x_1} = g_2^{PS'_i}.Y_1^{r_i} \quad (3)$$
  - The TA sends the pseudonym (PS_i, u_i) to its holder i.

C. Pseudonym's authenticity validation

Authenticity verification of generated pseudonyms is performed using our adapted version of the Camenisch's zero-knowledge proof of a Discrete Logarithm (PoK). Our version of the protocol allows nodes to produce encrypted TA's signatures of nodes identities while preserving their public verifiability. In other words, a given node holding a pseudonym PS_i can prove to any other node that its pseudonym is a valid TA's signature of its identity, without revealing the latter.

Given a pseudonym (PS_j, u_j) and the TA's public parameters (Y_1, Y_2, A), any node i in the IoT can verify the authenticity of PS_j as follows:

1) pseudonym holder j (Prover) randomly chooses secrets $m'_j, r'_j \in \mathbb{Z}_q$ and computes $u'_j = g_1^{r'_j}$, $e'_j = Y_1^{r'_j} g_2^{m'_j}$, $\gamma_j = g_2^{m'_j} Y_2^{m'_j}$.
2) j sends to node i (Verifier): (u'_j, e'_j, γ_j)
3) i chooses a challenge c and sends it to j.
4) j sends back to i : $\widehat{r_j} = r'_j - cr_j$, $\widehat{m_j} = m'_j - cPS'_j$, $\widehat{k_j} = m'_j + cH(ID_j||A)$.
5) i accepts the pseudonym PS_j if the following equalities hold:
$$u'_j =^{?} u_j^c g_1^{\widehat{r_j}}$$
$$e'_j =^{?} PS_j^c Y_1^{\widehat{r_j}} g_2^{\widehat{m_j}}$$
$$\gamma_j =^{?} g_2^{\widehat{m_j}} Y_2^{\widehat{k_j}} A^c$$

IV. Security Analysis

In this section, we analyze the security of proposed scheme with respect to required properties stated previously in this paper.

A. Adversary Model

We consider an adversary $\mathcal{A}$ which has the following capabilities: 1)

1) Eavesdrop and intercept exchanged traffic over non-secure wireless channel in the network.
2) Compromise one or more of nodes and obtain the secret information they hold.

Proposed scheme is said to be secure against above adversary model, if none of information obtained by $\mathcal{A}$ in 1) and 2), shall allow it to impersonate the TA or forge valid pseudonyms for unauthorized nodes.

B. Computational Diffie-Hellman and Discrete Logarithm assumptions

In our analysis, we consider the following computational problem assumptions:

a) Computational Diffie-Helman (CDH) assumption:: Let G be a cyclic group of order prime q with a generator g. CDH assumption states that, given (g, g^a, g^b) for random a, $b \in \mathbb{Z}_q^*$, there is no probabilistic polynomial-time algorithm that computes g^{ab} with non-negligible probability [14].

b) Discrete Logarithm Problem (DLP):: Let G be a cyclic group of order prime q with a generator g. DLP assumption states that, given (g, g^x) for random $x \in \mathbb{Z}_q^*$, it is hard to find x.

C. Node's anonymity disclosure

Theorem 1: *No one but the distributed TA can correctly match a pseudonym to corresponding identity within the protocol of pseudonym generation.*

Proof: Without loss of generality, assume a TA having generated a pseudonym PS_i for a given node i with identity ID_i. Suppose that, given the pseudonym (PS_i, u_i), an adversary $\mathcal{A}$ is able to guess corresponding identity ID_i with non-negligible probability.

In the first case, we assume that TA's signature PS_i' have been transmitted to i over a secure channel. In this case, the adversary computes $PS_i'^* = x_2^*.H(ID_i||A) + a^*$ and $PS_i^* = g_2^{PS_i'^*}.Y_1^{r_i^*}$. The adversary outputs the matching (PS_i, ID_i) if $PS_i^* = PS_i$. This matching would be correct if $x_2^* = x_2$ and $r_i^* = log_{g_1} u_i$. However, the adversary cannot reconstruct x_2 from $PS_i'^*$ with non-negligible probability, because the underlying Schnorr's signature scheme is proved to be secure under the random oracle model. Besides, $\mathcal{A}$ cannot either compute r_j^* considering the Discrete Logarithm Problem (DLP) assumption.

In the second case, we assume that the adversary $\mathcal{A}$ holds the secrets x_2 and a, in addition to intercepted TA's signature PS_i'. Hence, to match the pseudonym (PS_i, u_i) to its identity ID_i, the adversary proceeds as follows:

- Compute $PS_i' = x_2.H(ID_i^*||A) + a$ such that ID_i^* is randomly chosen identity.
- Compute $\lambda = Y_1^{r_i}$, given g_1, $Y_1 = g_1^{x_1}$ and $u_i = g_1^{r_i}$, where x_1 and r_i are unknown to $\mathcal{A}$.
- Compute $PS_i^* = g_2^{PS_i'}.\lambda$
- Outputs the matching (PS_i, ID_i^*) if $PS_i^* = PS_i$

However, the adversary would fail in computing correctly $\lambda = Y_1^{r_i}$ with non-negligible probability, considering the CDH assumption.

Therefore, we conclude that the probability that an adversary could match a pseudonym to corresponding identity is negligible.

Theorem 2: *Pseudonym verification protocol provides no information about the identity (ID_i) during verification of corresponding pseudonym PS_i.*

Proof: Pseudonym verification protocol is based on *Camenish*'s *Proof of Knowledge (PoK)* protocol [12], which is proven to be honest-verifier zero-knowledge protocol (kindly refer to [12] for details). That is, no useful information is revealed in the random oracle model. Therefore, because of the honest-verifier zero-knowledge property of underlying PoK, there is no information about ID_i is revealed.

From ***theorems*** **1** and **2**, we conclude that identity anonymity is guaranteed.

D. Pseudonym forgery

Theorem 3: *No one excepting the distributed TA could forge a valid verifiable pseudonym.*

Proof: Pseudonym unforgebility is ensured by verifiability property of pseudonym generation protocol. Indeed, a verifiable pseudonym PS_j is of the from $PS_j = E \circ S(ID_j)$, which is the verifiable encryption (E) [12] of the *Schnorr*'s signature (S) on identity (ID_j). The verifiability of PS_j is achieved by our pseudonym verification protocol (PVP) which is based on *Camenish*'s Proof of Knowledge (PoK) [12]. The latter is proven to be a verifiable encryption scheme, with respect to encryption function E, under RSA assumption [12]. That is, given a message M, the encryption $E(M)$ can be verified to be valid without revealing M. Accordingly, any pseudonym that is not an encryption under E should fail in PV protocol. On the other hand, given that *Schnorr*'s signature is proven to be secure in the random oracle model, no one can forge a valid signature $S(ID_j)$ without having PA's secret key x_2.

Assume an adversary $\mathcal{A}$ forges a pseudonym $PS_j^* = E \circ S(ID_j)^*$, where $S(ID_j)^* = x_2^*.H(ID_j||A^*) + a^*$, and ($x_2^*$, a^*) are randomly chosen. Given this, $\mathcal{A}$ cannot pass a valid execution of PV protocol, because the second equation in (**step 5**) cannot hold, and it is straightforward to verify this.

We conclude that, Pseudonym unforgebility is guaranteed.

E. Pseudonym impersonation

Theorem 4: *Given a verifiable pseudonym PS_j of node j, no one else can prove that its pseudonym is PS_j within pseudonym verification protocol.*

Proof: Given a pseudonym (PS_j, u_j) of node j with identity ID_j, assume that the matching (PS_j, ID_j) is known to an adversary $\mathcal{A}$. Assume that $\mathcal{A}$ impersonates j by issuing a message and claiming that it is signed by PS_j. This impersonation would be successful if $\mathcal{A}$ can perform a valid execution of the *Verifiable Pseudonym Protocol (PVP)* for the pseudonym PS_j. Suppose that PVP is executed between $\mathcal{A}$ (prover) and another node i (verifier).

Upon receiving ($u_j'^*$, $e_j'^*$, γ^*, γ'^*, α^*) from $\mathcal{A}$, node i sends a challenge c to $\mathcal{A}$ (**step 3** of PVP). The latter sends back to i : $(\widehat{r}_j^*, \widehat{m}_j^*)$ (**step 4**). i would accept PS_j only if the following equations hold (**step 5**), and hence this execution of the protocol would be valid:

$$u_j'^* =^? u_j^c \; g_1^{\widehat{r}_j^*}$$
$$e_j'^* =^? PS_j^c \; Y_1^{\widehat{r}_j^*} \; Y_2^{\widehat{m}_j^*} \; A^{-c}$$
$$\gamma'^* =^? \gamma^{*^c} \; \alpha^{*^{\widehat{m}_j^*}}$$

For the second equation to hold, the adversary should guess the challenge c in (**step 1**) to forge $e_j'^*$, such that the value of $e_j'^*$ validates the second equation. However, we can see that $\mathcal{A}$ cannot guess c before (**step 3**), and hence the check of second equation fails, because $\mathcal{A}$ cannot compute the right $e_j'^*$ without having challenge c. Assume now that $\mathcal{A}$, after receiving challenge c in (**step 3**), he forges $\widehat{r}_j^* = r_j'^* - cr_j^*$ and $\widehat{m}_j^* = m_j'^* - c.H(ID_j||A)$, where $r_j'^*$ and $m_j'^*$ are randomly chosen. Accordingly, when the verifier checks the second equation in (**step 5**), he finds the following:

$$\begin{aligned} e_j'^* &=^? PS_j^c \; Y_1^{\widehat{r}_j^*} \; Y_2^{\widehat{m}_j^*} \; A^{-c} \\ &= g_2^{cx_2.H(ID_j||A)+ca} \; Y_1^{cr_j} \; Y_1^{\widehat{r}_j^*} \; Y_2^{\widehat{m}_j^*} \; g_2^{-ca} \\ &= Y_2^{c.H(ID_j||A)} \; g_2^{ca} \; Y_1^{cr_j} \; Y_1^{r_j'^* - cr_j^*} \; Y_2^{m_j'^* - c.H(ID_j||A)} \; g_2^{-ca} \\ &= Y_2^{m_j'^*} \; Y_1^{cr_j} \; Y_1^{r_j'^* - cr_j^*} \end{aligned}$$

We can see that, this equation holds only if $e_j'^* = Y_2^{m_j'^*} \; Y_1^{r_j'^*}$ and $r_j^* = r_j$. However, $\mathcal{A}$ cannot guess r_j from $u_j = g_1^{r_j}$ assuming the DLP assumption, and hence the check of this equation fails. Consequently, we conclude that $\mathcal{A}$ cannot pass valid execution of PVP protocol for the pseudonym (PS_j, u_j), and hence it cannot impersonate PS_j's holder.

V. Conclusion

In this paper we suggested a solution to an important issue in IoT communication environment. We proposed a pseudonyms-based cryptographic solution for anonymous communications in IoT. Our approach is based on the concept of verifiable encryption to prevent adversaries to learn the identity attributes or any other user-related private information. Indeed, anonymity property of our approach provides privacy preserving to communicating objects in the IoT, where nodes communicate by using their pseudonyms rather than real identities. In addition, a significant highlight of our solution is the possibility for nodes to authenticate themselves or prove their membership party while they still be anonymous.

References

[1] S. Sicari, A. Rizzardi, L. A. Grieco, and A. Coen-Porisini, "Security, privacy and trust in internet of things: The road ahead," *Computer Networks*, vol. 76, pp. 146–164, 2015.

[2] R. Hervás, S. Lee, C. D. Nugent, and J. Bravo, Eds., *Ubiquitous Computing and Ambient Intelligence. Personalisation and User Adapted Services - 8th International Conference, UCAmI 2014, Belfast, UK, December 2-5, 2014. Proceedings*, ser. Lecture Notes in Computer Science, vol. 8867. Springer, 2014.

[3] P. N. Mahalle and P. N. Railkar, "Identity management for internet of things," *River Publishers Wharton*, 2015.

[4] M. M. Hossain, M. Fotouhi, and R. Hasan, "Towards an analysis of security issues, challenges, and open problems in the internet of things," in *2015 IEEE World Congress on Services, SERVICES 2015, New York City, NY, USA, June 27 - July 2, 2015*, 2015, pp. 21–28.

[5] M. Elkhodr, S. A. Shahrestani, and H. Cheung, "The internet of things: New interoperability, management and security challenges," *CoRR*, vol. abs/1604.04824, 2016.

[6] D. Huang, "Pseudonym-based cryptography for anonymous communications in mobile ad hoc networks," *IJSN*, vol. 2, no. 3/4, pp. 272–283, 2007.

[7] L. B. Oliveira, A. Kansal, C. P. L. Gouvêa, D. F. Aranha, J. López, B. Priyantha, M. Goraczko, and F. Zhao, "Secure-tws: Authenticating node to multi-user communication in shared sensor networks," *Comput. J.*, vol. 55, no. 4, pp. 384–396, 2012.

[8] K. Shim, Y. Lee, and C. Park, "EIBAS: an efficient identity-based broadcast authentication scheme in wireless sensor networks," *Ad Hoc Networks*, vol. 11, no. 1, pp. 182–189, 2013.

[9] D. Evans and D. M. Eyers, "Efficient data tagging for managing privacy in the internet of things," in *2012 IEEE International Conference on Green Computing and Communications, Conference on Internet of Things, and Conference on Cyber, Physical and Social Computing, GreenCom/iThings/CPSCom 2012, Besancon, France, November 20-23, 2012*, 2012, pp. 244–248.

[10] D. Huang, S. Misra, M. Verma, and G. Xue, "PACP: an efficient pseudonymous authentication-based conditional privacy protocol for vanets," *IEEE Trans. Intelligent Transportation Systems*, vol. 12, no. 3, pp. 736–746, 2011.

[11] T. Gao and X. Deng, "A pseudonym ring building scheme for anonymous authentication in vanets," in *Advances on Broadband and Wireless Computing, Communication and Applications*, L. Barolli, F.-Y. Leu, T. Enokido, and H.-C. Chen, Eds. Springer International Publishing, 2019, pp. 481–489.

[12] J. Camenisch and V. Shoup, "Practical verifiable encryption and decryption of discrete logarithms," in *Advances in Cryptology - CRYPTO 2003, 23rd Annual International Cryptology Conference, Santa Barbara, California, USA, August 17-21, 2003, Proceedings*, 2003, pp. 126–144.

[13] C.-P. Schnorr, "Efficient identification and signatures for smart cards," in *Proceedings of the 9th Annual International Cryptology Conference on Advances in Cryptology*. Springer-Verlag, 1990, pp. 239–252.

[14] W. Diffie and M. E. Hellman, "New directions in cryptography," *IEEE Trans. Information Theory*, vol. 22, no. 6, pp. 644–654, 1976.

Chaotic Encryption for Fingerprint images

Ahmed SABRI
LMSE Lab. Electronics Dept.
USTO, Oran, Algeria
ahmedustopg@hotmail.com

Mohamed OUSLIM
LMSE Lab. Electronics Dept.
USTO, Oran, Algeria
ouslim@yahoo.com

***Abstract*—To protect the transmission of biometric information over computer networks, the cryptography is considered as the adequate solution. In this paper, we propose another encryption method for the fingerprint data. We start by giving details of the encryption process, where both encryption sub-processes, namely, confusion and diffusion, utilize the new multimodal Piece-Wise Linear Chaotic Map (PWLCM). This technique is examined using several tests on a standard fingerprint database. The obtained results are given together with deep examination, to show that the proposed encryption method is highly secure, due mainly to its vast key's space and the perfect effect of the two encryption sub-processes. Moreover, as clearly indicated by the results, we demonstrated that this method has successfully passed the National Institute of Standards and Technology Special Publication 800-22a tests and security examinations, which affirms that the proposed method is a good cryptographic system to secure fingerprint images.**

Keywords—Security, Cryptography, Chaotic Encryption, PWLC map, Fingerprint images.

I. INTRODUCTION

It is considered that a particular issue identified by the security of biometric systems against attacks, is their insurance of biometric data when these formats are stored in a database or transmitted over computer networks. Our work depends on the fingerprint image as a processed biometric data since the unique mark methodology isn't nosy, which implies it doesn't achieve the intimacy of the person. Likewise, fingerprints are distinctive among people and even between the fingers of the same person. The details are the novel highlights of fingerprints, which include the position, orientation and type, and so on. These details can group fingerprints into whorls, circles and curves [1].

Biometric information security is a touchy issue where the security of a fingerprint data sent over the Internet networks and its accessibility in the open system condition, which turns into a crucial issue [2]. Jain et al. [3] demonstrate that the best biometric system must ensure the biometric information of the real individual in the enrollment process. Besides, despite the fact that biometrics guarantees the uniqueness, it doesn't guarantee privacy on the grounds that our fingerprints are left on anything we contact with fingers. Subsequently, encryption demonstrated its effectiveness to improve the security of fingerprint information [4].

The use of conventional encryption methods to anchor the fingerprint images, are inadmissible for practical utilization [5] in view of the real proprieties of these images, including the high correlation among pixels [6]. Subsequently, the field of utilization for traditional encryption systems, was extremely restricted and unsuitable, which raised reasonable concerns [7]. With essential research in the field, ongoing encryption procedures are demonstrating [8] where the most consideration was attracted by the chaotic encryption [9].

II. RELATED WORKS

The work depicted in this paper comprises basically two parts. These are the biometric cryptosystem and chaotic encryption. Several research works exist in this field.

A. Biometric Encryption

We carried out a detailed bibliographic study on different biometric cryptosystems existing in the literature [10-20]. We can quote Soutar and Tomko, in 1996, who have structured an encryption algorithm for fingerprint images dependent on Fourier transformation and a DES-like algorithm [10]. Soutar et al. [11] additionally utilized the Fourier transformation in their origination of a private encryption method for biometric data. Ratha et al. [12] used a unique alteration in the frequency transformation of biometric images in their encryption method. Similarly, a biometric encryption method was proposed in [13] with the direct use of extraordinary transformation to the biometric images. In our case, and as a result of this study, we concluded that current trends will benefit the chaotic encryption.

B. Chaotic Encryption

The utilization of chaotic systems is the most recent methodology for the encryption techniques. This method began in 1989 as the primary recommendation [21]. These cryptosystems are not the same as others with their special characteristics, for example, control parameters, non-convergence, sensitivity to initial conditions and non-periodicity [22], [23]. The security level and the simplicity are the primary points of interest of a 1-D chaotic cryptosystem [24], and many works [25], [26], [27], [28] were done to prove it. Recently, the fingerprint cryptosystems have used the chaotic generators to enhance the security [29], [30], [31]. Han et al. [29] used in their fingerprint cryptosystem a 2-D chaotic map considering initial values of the chaotic generator as the encryption key. This generation of chaotic sequences was based on the distribution of binary pixels extracted from fingerprint images. Another fingerprint encryption scheme was proposed by Zhao et al. [30], where they merge a nonlinear chaotic system with shuttle operation. Hsiao et al. [18], have designed recently a fingerprint encryption system using a multiple chaotic generator based on two 3-D and two 1-D chaotic maps.

The cited literature here indicated that the preceding researches concentrated mainly on multiple chaotic maps. Our objective therefore, is to contribute to the enhancement of this idea, by merging chaotic maps. This paper presents a new cryptographic system by using a new multimodal PWLCM maps to improve the cryptographic security strength of the fingerprint image.

In the following sections, we introduce the chaotic maps employed and we present the proposed fingerprint cryptosystem in section III. The experimental results and the security analyses are presented in section IV and section V, respectively. The conclusion is given in section VI.

III. The Proposed Chaotic Encryption

This research work proposes a new chaos-based encryption scheme for fingerprint images using the two efficient processes of permutation and diffusion, which both use a new chaotic map. In the permutation process, a chaotic multimodal PWLCM is used with a variant control parameter for every iteration, where the control parameter values are generated from the pixels values of the processed fingerprint image. In the diffusion process, a second new multimodal PWLCM map with fixed intervals is used to generate a different sequence of grey values. This chaotic sequence is applied to change the pixel grey values of the fingerprint image after the permutation process. This chaos-based image encryption shows big sensitivity to both the initial conditions and the control parameters of the used chaotic systems. In addition, the encryption scheme presents good dependence on the plain fingerprint image. Hence, this chaotic scheme presents a big resistance to several known attacks such as statistical and differential attacks. Furthermore, this encryption system, characterized by the large space of the values of the key, is very strong against the brute-force attack.

A. The Multimodal PWLCM Map

In this paper, we use a chaotic system with more advantages compared to the skew tent map [32]. This system is based on the PWLCM map which was proposed by Zhou [33]. This map is extensively used for chaos generation due to its perfect properties, such as a uniform invariant density function, exactness, mixing and ergodicity, an exponentially decaying correlation function. The mathematical definition of the unimodal PWLCM map is given by equation 1.

$$x(s+1) = f_{PWLCM}(x(s)) \tag{1}$$

Where, $f_{PWLCM}: [0,1] \rightarrow [0,1]$ is defined by equation (2).

$$f_{PWLCM}(x) \begin{cases} \frac{x}{p} & 0 \le x \le p \\ \frac{x-p}{0.5-p} & p < x \le 0.5 \\ f_{PWLCM}(1-x) & 0.5 < x \le 1 \end{cases} \tag{2}$$

Where $p \in]0,0.5[$ is the control parameter, and $x \in [0,1]$ is the state of the system.

An extent of the regular PWLCM map (2) is shown in this work to create a multimodal PWLCM map, $f_{PWLCM}: [0,1] \rightarrow [0,1]$, based on two ways. The first one deals with the permutation process, using one variant control parameter by changing the control parameter p in every iteration, as it is shown in equation (3). The second way is for the diffusion process where we use several fixed control parameters for all iterations, as it is shown in equation (4).

$$x_{i+1} = \begin{cases} \frac{x_i}{p_i} & 0 \le x_i \le p_i \\ \frac{x_i - p_i}{0.5-p_i} & p_i < x_i \le 0.5 \\ f_{PWLCM}(1-x_i) & 0.5 < x_i \le 1 \end{cases} \tag{3}$$

Where $i = 0, \dots, N-1$ and N is the length of the generated orbit which is the size of the processed image.

$$x_{i+1} = \begin{cases} \frac{x_i - p_{2k}}{p_{2k+1} - p_{2k}} & p_{2k} \le x_i \le p_{2k+1} \\ \frac{p_{2k+2} - x_i}{p_{2k+2} - p_{2k+1}} & p_{2k+1} < x_i \le p_{2k+2} \\ f_{PWLCM}(1-x_i) & 0.5 < x_i \le 1 \end{cases} \tag{4}$$

Where $k = 0, \dots, n-1$; $0 = p_0 < p_1 < \cdots < p_{2n-1} < p_{2n} = 0.5$ and n define the number of fixed control parameters.

B. Permutation Process

The pixel's values of the fingerprint image are used to calculate the control parameter p of the first multimodal PWLCM map (3) in every iteration, to generate the next system state x_{i+1}which will be used for the XOR operation with the next processed pixel. The new pixel's value is used to calculate the next control parameter p, this operation will be repeated until we finish the permutation process for all image pixels. As the initial value for the multimodal PWLCM map (3), we will use $x_1 \in [0,1]$ which is the part one of the encryption key. We can describe the permutation process with the following four steps.

- Step one: Set the initial condition x_1 for the multimodal PWLCM map (3).
- Step two: Iterate the multimodal PWLCM map (3) M iterations. M is an integer representing the part three of the encryption key.
- Step three: For every pixel of the processed image defined by 〚 px〛_i,i=0,1,…,H×W with H,W are respectively, the height and the width of the fingerprint image:
  - Calculate the control parameter p_i using the pixel value px_i with $p_i = px_i/512$.
  - Generate the next state x_{i+1} of the multimodal PWLCM map (3) using p_i with $x_{i+1} = f_{pwlcm}(x_i, p_i)$.
  - Xor the pixel value px_{i+1} with x_{i+1}; the result is the permuted pixel and it is used as px_i in the next iteration; $px_{i+1} = px_{i+1} \otimes x_{i+1}$.

Starting with the specific initial value $x_0 = 0.4567890$, a chaotic sequence was generated from the proposed multimodal PWLCM system (3), which is used for the permutation process. This system needs the processed fingerprint image for the orbit generation. So, the fingerprint images, shown in Fig. 1a, are used to generate four different orbits. For the processed fingerprint images, the waveforms for the generated sequences given in Fig. 1b of $H \times W$ elements, are quite irregulars, indicating the chaotic state of the proposed multimodal PWLCM system (3). In the case of the generated typical orbits with length $H \times W = 241920$, the data distribution is shown in the histograms of Fig. 1c. In this figure, we can see the uniform distribution of the data elements for the four generated orbits, over the unit interval during time.

Furthermore, the multimodal PWLCM with a variant control parameter (3) has desirable correlation's properties. The generated orbits are used to calculate the auto-correlation coefficients, which are shown in Fig. 1d. The cross-

correlation is calculated between the four generated sequences and represented by Fig. 1e. This figure indicates that the system is very sensitive in the case of the processed image. Consequently, we can state that there is a tight relationship between the generated orbit from the chaotic system (3) and the fingerprint image after the permutation.

Fig. 1a. Processed images with $H \times W = 480 \times 504$.

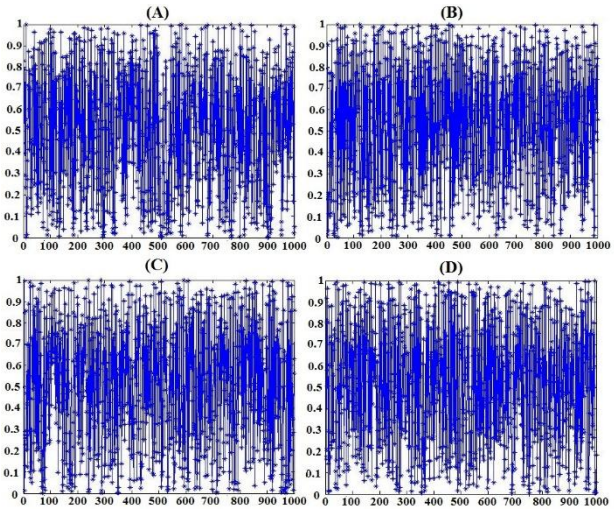


Fig. 1b. The related chaotic orbits for $x_0 = 0.4567890123456789$.

C. Diffusion Process

In the diffusion process, the second multimodal PWLCM (4) is used where a sequence of length $H \times W$ is generated, then Xored with the permuted fingerprint image. The diffusion operation is outlined by the following four steps.

- Step one: Set the control parameters values b_i and x_2 for the multimodal PWLCM map (4), where $x_2$is the second part of key encryption.
- Step two: Iterate the multimodal PWLCM (4) M iteration.
- Step three: Generate a sequence with length $H \times W$.
- Step four: Xor the chaotic sequence with the permutated image.

Two chaotic sequences, starting with the values of $x_0 = 0.567891234567891$ and $y_0 = 0.567891234567892$ are generated with the second multimodal PWLCM (4), for $n = 3$ and $b_i = [0,0.16,0.3,0.41,0.5]$. The results for the distribution of points and correlation coefficients are presented with more details in [48].

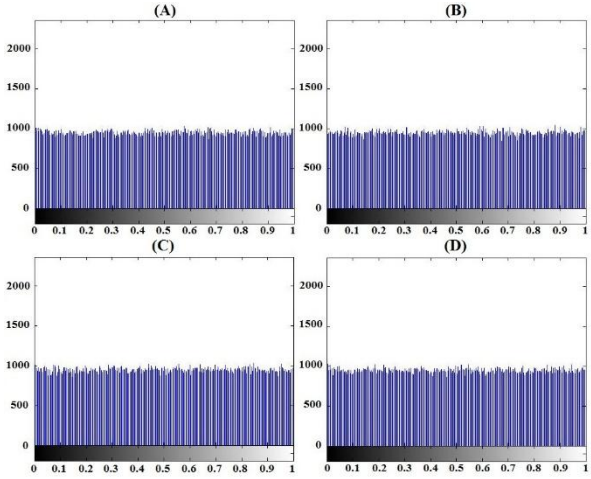


Fig. 1c. The related orbits histograms with length $H \times W = 241920$.

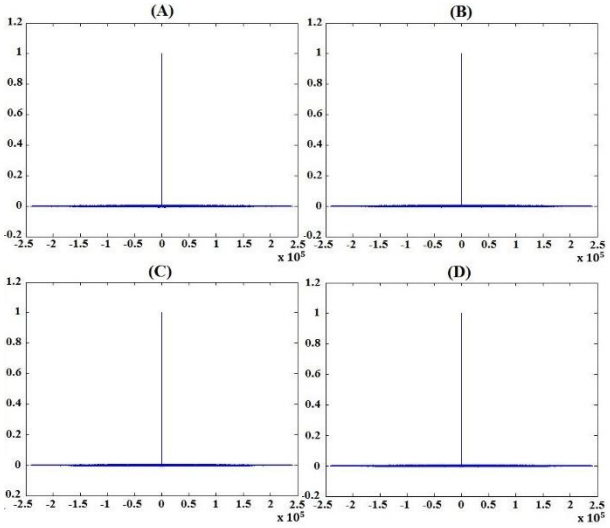


Fig. 1d. The related auto-correlation.

IV. Exprimental Results

Several simulation tests were carried out on a PC workstation. In this section, the obtained results are illustrated. The manipulated images are taken from a standard fingerprint database called, Cross Match Sample database "VeriFinger_Sample_DB" [34], which contains hundreds of TIFF fingerprint images with size $H \times W = 480 \times 504$. The four fingerprints images shown in Fig. 1a are used as the plain images and Fig. 3a show their encrypted images respectively. The histograms of the plain images and their encrypted images are shown in Fig. 3b and Fig. 3c respectively. The computed precision is around 10^{-16} for the encryption process. The encrypted conditions for the chaotic systems were set up as follows.

- The proposed multimodal PWLCM map (3): $x_1 = 0.4567890123456789$.
- The proposed multimodal PWLCM map (4): $x_2 = 0.8901234567890123$ and $b_i = [0,0.16,0.3,0.41,0.5]$.
- For all chaotic systems, the parameter M=1000 iterations.

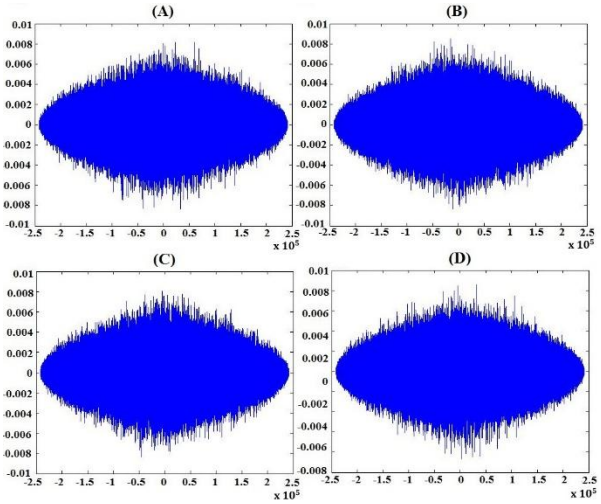


Fig. 1e. The correlation between the generated orbits.

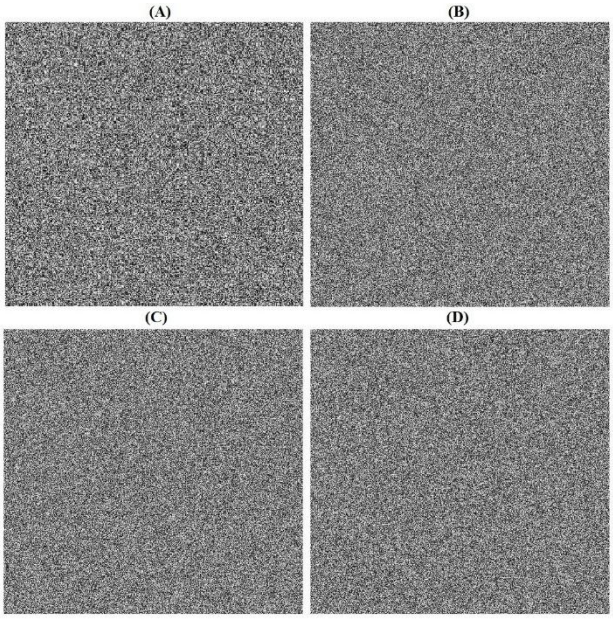


Fig. 3a. The encrypted images for the originals of Fig. 1a, respectively.

V. Performance and Security Analysis

In this part, we perform some deep analysis on the proposed fingerprint image encryption method, to highlight its security. We chose then, the most important tests such as, the differential, statistical and the key space analysis [35]. The results of these tests indicate the high security of the proposed fingerprint image encryption.

A. Secret Key Sspace

In order to achieve the best resistance to the brute-force attacks, the encryption system should have a large key space.

The key space of the proposed encryption system is the combination of different parameters used as initial conditions in this chaotic system. As mentioned previously, the encryption key in the proposed technique is composed of four parts x_1, x_2, M, b_i. For b_i, the number of parameters is not fixed. In our work, we consider five parameters for b_i. Thus; the secret key used in the proposed technique is composed of a total of eight parameters. If the computed precision is 10^{-16}, for all parts and 10^{5} for M, then we will have a key space of approximately $10^{16\times7} \times 10^{5} \approx 2^{400}$. This key may be represented with more than 412 bits, which is fairly enough to resist to an exhaustive attack [36].

The comparison results between the secret key spaces of the proposed method with other algorithms are shown in TABLE I, in which we can clearly see that the secret key space of the proposed algorithm is much better than that of other schemes.

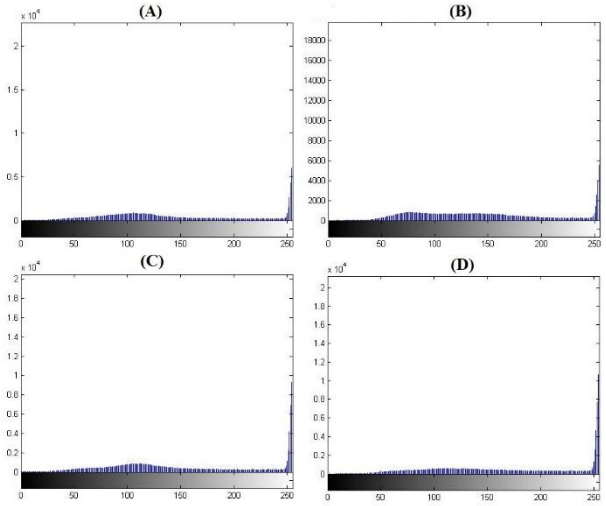


Fig. 3b. Histograms of the original images of Fig. 1a, respectively.

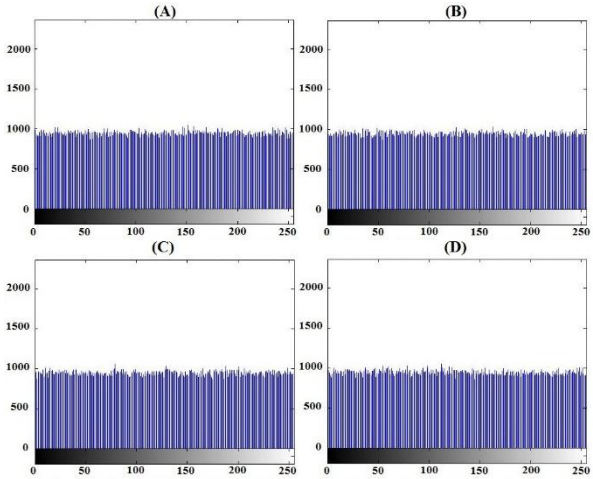


Fig. 3c. Histogram of the encrypted images, respectively.

B. Secret Key Sensitivity Analysis

The sensitivity to the secret key is an essential characteristic for a good cryptosystem that ensures safety against any exhaustive attack. In this part, we carried out two types of test to observe the sensitivity effect on the secret key of our encryption method.

TABLE I. COMPARISON OF SECRET KEY SPACE

Encryption Algorithms	Secret Key Space
Proposed method	$\approx 2^{400}$
A.SABRI [48]	$\approx 2^{600}$
Hsiao & Lee [37]	$\approx 2^{512}$
Bhatnagar & Wu [16]	$\approx 2^{280}$
Liu [39]	$\approx 2^{240}$
Wang & Zhang [38]	$\approx 2^{236}$
Zhou et al. [40]	$\approx 2^{225}$

- Test one: In the first step, the fingerprint image, given Fig. 1a. (B), is encrypted using an original secret key. In the second step, the same image is encrypted using other slightly different keys. The TABLE II shows the secret keys used for encryption, taking into consideration that for every key we slightly change just one part, whereas the other parts stay the same as the original key. The obtained results of correlation between the encrypted-image using the original key and the other encrypted-images are shown in TABLE III. It is clear that there is a strong de-correlation between the first encrypted image with the original key and the other encrypted images with slightly different keys.
- Test two: Similarly, the fingerprint image in Fig. 1a. (B) is encrypted with the original secret key of TABLE II. In the second step, we try to decrypt the encrypted image with the other slightly different keys of TABLE II. The result of correlation between the decrypted images and the original image is shown in TABLE IV. The sensitivity test can also be visually demonstrated by the Fig. 4. From TABLE IV, a strong de-correlation is obtained between the pixels of the original image and the images decrypted by the other slightly different keys. Therefore, we can state that the proposed algorithm is sensitive to any small change in the secret key.

TABLE II. THE DEFERENT SECRET KEYS USED FOR ENCRYPTION

Original key	Key X
$x_1 = 0.45$	Key 1, $x_1 + 10^{-16}$
$x_2 = 0.89$	Key 2, $x_2 + 10^{-16}$
$b_1 = 0.00$	Key 3, $b_1 + 10^{-16}$
$b_2 = 0.16$	Key 4, $b_2 + 10^{-16}$
$b_3 = 0.30$	Key 5, $b_3 + 10^{-16}$
$b_4 = 0.41$	Key 6, $b_4 + 10^{-16}$
$b_5 = 0.50$	Key 7, $b_5 - 10^{-16}$
M=1000	Key 8, $M + 1$

TABLE III. CORRELATION BETWEEN THE ENCRYPTED IMAGE USING ORIGINAL KEY AND THE OTHER ENCRYPTED IMAGES

Keys	Correlations
Key 1	-0.0007
Key 2	$+0.0054$
Key 3	-0.0004
Key 4	-0.0004
Key 5	$+0.0035$
Key 6	-0.0003
Key 7	-0.0011
Key 8	-0.0007

TABLE IV. CORRELATION BETWEEN THE ORIGINAL IMAGE AND DECRYPTED IMAGES WITH THE SLIGHTLY DIFFERENT KEYS.

Keys	Correlations
Key 1	$+0.0387$
Key 2	$+0.0001$
Key 3	$+0.0024$
Key 4	$+0.0023$
Key 5	$+0.0011$
Key 6	$+0.0005$
Key 7	-0.0015
Key 8	$+0.0004$

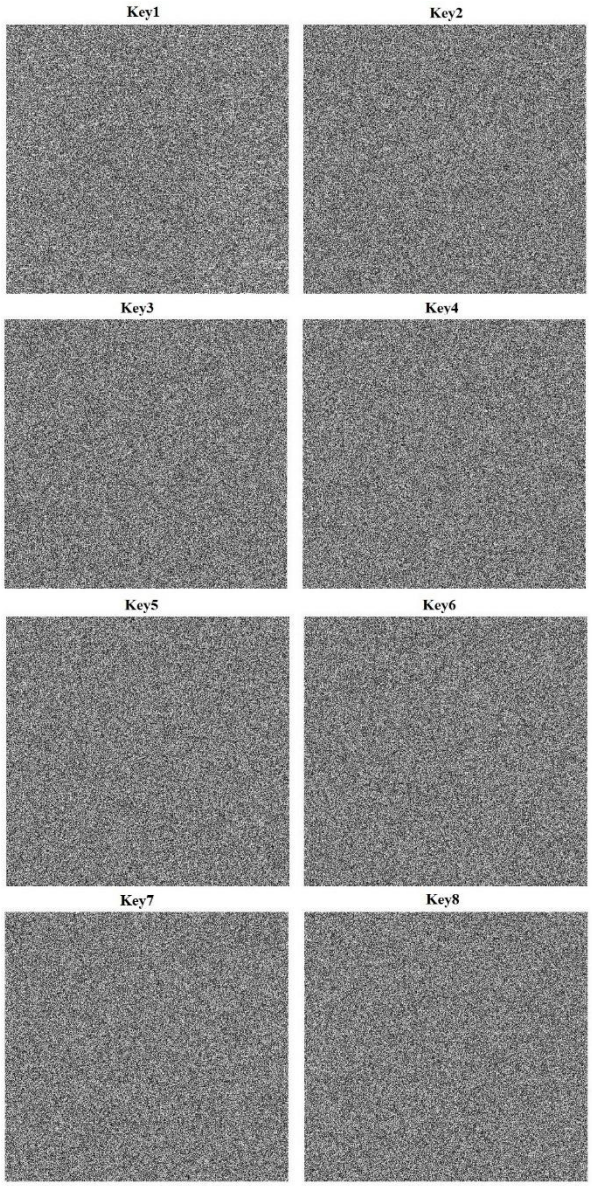


Fig. 4. The decrypted images with the eight slightly different keys.

C. Statistical Analysis

The work of Shannon [41] shows that a lot of categories of encryption systems are able to be broken by the statistical attacks. Consequently, the fact to resist to the statistical tests on the encrypted image presents a highly desirable advantage to the encryption system. In this part, we applied the following statistical tests to prove the high robustness of the proposed encryption system.

a) Histogram Analysis: In the image encryption system, any modification in the distribution features should be taken into consideration. If attackers get access to the original image histogram, their statistical attack will be of high performance, therefore, the good encryption system must cover all original pixel's values and generates a flat histogram with uniform distribution.

In this analysis, the fingerprint images shown in Fig 1a are encrypted, and then we generate the histograms for both the originals and their encrypted versions shown respectively in Fig. 3b and Fig. 3c. Fig. 3c indicates high uniform distribution in the histograms of the encrypted images, which are very different from the originals. We conclude therefore that the encrypted image's histogram cannot be useful to apply any statistical attacks.

b) Correlation Analysis: The simple way to calculate the correlation between adjacent pixels, is to randomly select several adjacent pixel pairs, and then to calculate the corresponding correlation coefficients. In this paper, we have limited the group size to 2000 pairs of adjacent pixels, taken from three directions of the image. These are, the vertical, horizontal and the diagonal. We tested the correlation between adjacent pixels in both the encrypted and the original images, separately. TABLE V shows that the means of the calculated correlations of adjacent pixels in all directions are very close to one for the original image. Even more, the calculated correlations corresponding to the ciphered image are close to zero. Therefore, the condition of zero correlation [42] is respected by the proposed encryption scheme.

Fig. 5 shows the correlation distribution analysis of two adjacent pixels in the vertical, horizontal, and diagonal positions for respectively the plain image given in Fig. 1a. (A) and its ciphered version given in Fig. 3a. (A). we can see that the correlations between adjacent pixels are completely broken in the three directions of the encrypted images.

TABLE V. CORRELATION COEFFICIENTS OF TWO ADJACENT PIXELS IN DIFFERENT ORIGINAL AND ENCRYPTED IMAGES.

	correlation	vertical	horizontal	diagonal
Original images	Fig. 1a. (A)	0.9119	0.9035	0.8345
	Fig. 1a. (B)	0.8754	0.9354	0.8404
	Fig. 1a. (C)	0.8690	0.8962	0.8182
	Fig. 1a. (D)	0.8319	0.8832	0.7264
Encrypted images	Fig. 3a. (A)	0.0326	0.0063	0.0050
	Fig. 3a. (B)	-0.0155	-0.0149	-0.0101
	Fig. 3a. (C)	-0.0199	0.0328	-0.0146
	Fig. 3a. (D)	0.0272	-0.0041	-0.0428

D. Differential Analysis

In order to measure the effect of a small change of the original image on its encrypted one, the number of pixel change rate (NPCR) and the unified averaged changing intensity (UACI) are used. The NPCR is used to calculate the percentage of different pixel numbers between two encrypted images and the UACI to measure the average intensity differences between these two images. To get a good encryption system, the values of NPCR and UACI should be large enough to resist against the differential attacks. We randomly chose one pixel and change the grey values with a difference of one, in the original images shown in Fig. 1a. The calculated values of NPCR and UACI are giving in TABLE VI.

Table VII shows the comparison of NPCR and UACI with the proposed scheme and other methods using the mean of the calculated values for the images of Fig. 1a. We can notice that the NPCR exceeds 99% and the UACI is above 33% for the proposed scheme, which can satisfy the level of security requirement [43]. The proposed algorithm shows extreme sensitivity to the plain text. Therefore, the algorithm is resistant to a differential attack.

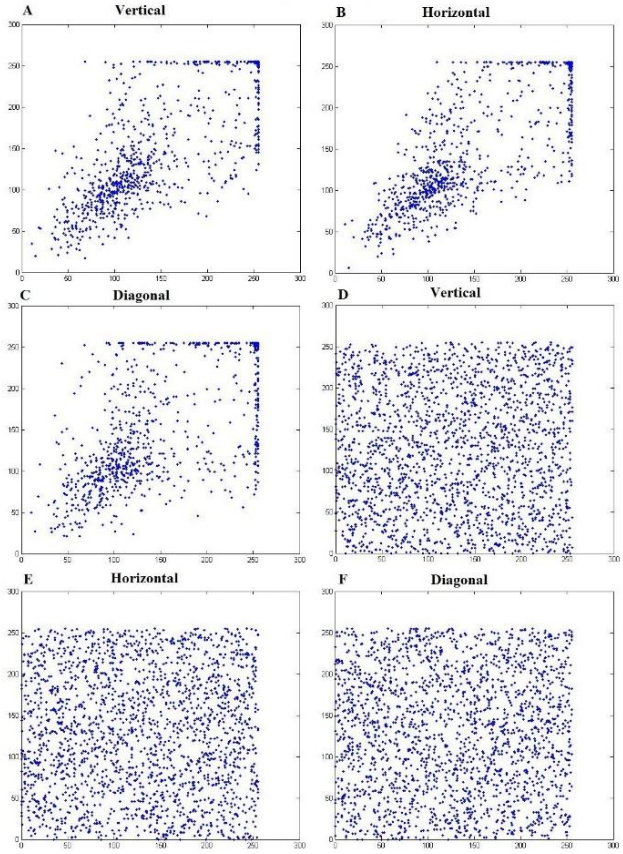


Fig. 5. Correlation analysis of two adjacent pixels: (A)–(C) are for the original image of (Fig. 1a. (A)); (D)–(F) are for the encrypted image (Fig. 3a. (A)).

TABLE VI. THE NPCR AND UACI FOR DIFFERENT IMAGES

Image	NPCR %	UACI %
Fig. 1a. (A)	99.6044	33.5101
Fig. 1a. (B)	99.6131	33.5482
Fig. 1a. (C)	99.6152	33.4451
Fig. 1a. (D)	99.5912	33.5642

TABLE VII. THE COMPARISON OF NPCR AND UACI WITH OTHER METHODS

Image	NPCR %	UACI %
The proposed scheme	99.605975	33.516900
A.SABRI[48]	99.505525	33.345575
Hsiao & Lee [37]	99.524618	33.325924
Zhang and Wang [44]	99.602781	33.295821
Wu et al [45]	99.552798	33.382791

E. Information Entropy Analysis

In order to measure the randomness of an information source m, we can use the information entropy $H(m)$ which is given in equation (5).

$$H(m) = \sum_{i=0}^{T-1} p(m_i) \log_2 \frac{1}{p(m_i)} \quad (5)$$

Where T is the total number of symbols $m_i \in m$; $p(m_i)$ denotes the probability of symbols. The theoretical value of the information entropy, for a source sending out 256 symbols, is $H(m) = 8$. The values of the information entropy close to 8 indicate the high robustness of the encrypted image against attacks [46]. In this analysis, we calculate the information entropies corresponding to the different encrypted images shown in Fig. 3a. The results are listed in TABLE VIII. This table illustrates that the entropy's values are close to 8, which indicates that the proposed algorithm possesses a good property of the information entropy.

F. NIST Randomness Tests for Encrypted Images

The generation of random images must be guaranteed by the good encryption system. Hence, we must verify the randomness of the encrypted images by the proposed method. We have used the NIST SP800-22a Test Suite [47] for checking the randomness of the encrypted images. The NIST SP800-22a statistical test is used to calculate the p-value, if the p-value is equal to one, then the tested sequence is perfectly random, on the other hand a p-value of zero shows the non-randomness. A significance level α is set to determine the acceptance of the hypothesis of randomness for a given sequence. Typically, α is chosen in the range [0.001, 0.01].

TABLE VIII. THE RESULTS OF INFORMATION ENTROPY

Encrypted images	Shannon entropy
Fig. 3a. (A)	7.9993
Fig. 3a. (B)	7.9993
Fig. 3a. (C)	7.9992
Fig. 3a. (D)	7.9992

To perform this test, the conversion of the encrypted images to binary sequences was applied and the parameter α was set to 0.01. TABLE IX shows the obtained results, where all sub-tests are passed by the binary sequences which indicate the randomness of the encrypted images. Therefore, the safety and robustness of the proposed encryption system are fulfilled.

TABLE IX. NIST SP 800-22A RANDOMNESS TESTS FOR ENCRYPTED IMAGES

NIST SP 800-22a tests name	Encrypted image Fig. 3a. (A)	Encrypted image Fig. 3a. (B)	Encrypted image Fig. 3a. (C)	Encrypted image Fig. 3a. (D)	Results
Frequency Monobit	0,092841	0,619905	0,190301	0,379728	Success
Frequency test within a block	0,345826	0,782000	0,703346	0,738977	Success
Runs test	0,249854	0,715124	0,341137	0,086164	Success
Longest run of ones in a block	0,349129	0,486873	0,639591	0,469785	Success
Binary matrix rank	0,115928	0,335806	0,385659	0,211635	Success
Discrete fourier transform (spectral)	0,746528	0,766592	0,182709	0,702025	Success
Non overlapping template matching	0,035379	0,014090	0,248254	0,064469	Success
Overlapping template matching	0,577844	0,017442	0,666520	0,502344	Success
Maurer's “universal statistical” test	0,698739	0,365429	0,450743	0,256632	Success
Linear complexity	0,153029	0,904322	0,836905	0,973007	Success
Serial P-value 1	0,385925	0,520010	0,247425	0,318415	Success
Serial P-value 2	0,558798	0,477092	0,181074	0,310840	Success
Approximate entropy	0,469091	0,063959	0,679386	0,750887	Success
Cumulative sums forward	0,117576	0,773474	0,119708	0,603896	Success
Cumulative sums reverse	0,078909	0,359521	0,186240	0,438627	Success
Random excursions X= -4	0,150222	0,888254	0,779025	0,279875	Success
Random excursions X= -3	0,772717	0,996753	0,577283	0,195268	Success
Random excursions X= -2	0,050793	0,373688	0,629799	0,359301	Success
Random excursions X= -1	0,741397	0,944197	0,944039	0,295721	Success
Random excursions X= 1	0,779159	0,517450	0,890934	0,970334	Success
Random excursions X= 2	0,135607	0,377322	0,867061	0,816850	Success
Random excursions X= 3	0,654772	0,585036	0,608576	0,513759	Success
Random excursions X= 4	0,964748	0,973495	0,797535	0,569354	Success
Random excursions variant X= -9	0,760647	0,202352	0,783388	0,379297	Success
Random excursions variant X= -8	0,900453	0,195840	0,722311	0,680702	Success
Random excursions variant X= -7	0,992058	0,250194	0,421466	0,951621	Success
Random excursions variant X= -6	0,841345	0,261202	0,291631	0,509538	Success
Random excursions variant X= -5	0,636567	0,259754	0,170390	0,364803	Success
Random excursions variant X= -4	0,755065	0,395992	0,090023	0,611530	Success
Random excursions variant X= -3	0,624494	0,566039	0,192418	0,910979	Success
Random excursions variant X= -2	0,300225	0,568732	1,701501	0,226729	Success
Random excursions variant X= -1	0,281663	0,335823	0,948357	0,110992	Success
Random excursions variant X= 1	0,306420	0,674829	0,673754	0,851268	Success
Random excursions variant X= 2	0,330159	0,530717	0,970170	0,800584	Success
Random excursions variant X= 3	0,282252	0,274566	0,850659	0,685266	Success
Random excursions variant X= 4	0,377968	0,143080	0,995116	0,611530	Success
Random excursions variant X= 5	0,792422	0,057404	0,737895	0,917037	Success
Random excursions variant X= 6	0,931020	0,070694	0,732537	0,644304	Success
Random excursions variant X= 7	0,885248	0,065306	0,882183	0,690121	Success
Random excursions variant X= 8	0,788153	0,025472	0,682009	0,840137	Success
Random excursions variant X= 9	0,610634	0,018185	0,527202	0,987905	Success

VI. Conclusion

In this paper, an encryption algorithm based on new chaotic maps is proposed, implemented and applied to the biometric fingerprint images in order to secure their transmission within computer networks. An efficient shuffling of image pixels is used by this encryption system in the permutation process. In the diffusion operation, the proposed scheme makes a total change to the pixel grey values. The proposed method has successfully passed several security tests, which confirm its robustness against different attacks. In addition, the NIST SP 800-22a tests presented here prove its good randomness characteristic.

All the experimental results show that the proposed encryption scheme is secure, and it is recommended for transmission of biometric images in computer networks.

However, the main drawback of this method is its key space, which is considered very high and makes its management and its storage practically difficult.

Nomenclature

b_i	Control parameters of the PWLCM map.
CB_j	Code book of the control parameters.
DES	Data Encryption Standard.
f_{PWLCM}	PWLCM function.
H	Height of the fingerprint image.
H(m)	Information entropy.
m	Information source.
m_i	Symbols of the information source m.
M	Number of iterations.
N	Length of the chaotic orbit.
NIST	National Institute of Standards & Technology.
NPCR	Number of Pixel Change Rate.
PWLCM	Piece Wise Linear Chaotic Map.
$p(m_i)$	Probability of symbols for the source m.
p-value	Probability of the NIST-SP800-22a tests.
px_i	Processed pixel value.
PWLCM	Piece Wise Linear Chaotic Map.
T	Total number of symbols m_i.
UACI	Unified Averaged Changing Intensity.
W	Width of the fingerprint image.
α	Threshold for the accepted p-values.

Acknowledgment

This work was supported by university of Science and Technology-Oran, Algeria.

References

[1] H. Chen, A novel algorithm of fingerprint encryption using minutiae based transformation, *Pattern Recognit. Lett*, Vol. 32, no. 2, pp. 305-309, 2011.

[2] T. Ahmad, J. Hu, and S. Wang, Pair-polar coordinate-based cancellable fingerprint templates, *Pattern Recognit. Lett*, Vol. 44, no. 10, pp. 2555-2564, 2011.

[3] K. Jain, A. Ross, and S. Pankanti, Biometrics: A tool for information security, *IEEE Trans. Inform. Forensics Sec.*, Vol. 1, pp. 125-143, 2006.

[4] G. Bhatnagar, Q.M.J. Wu, B. Raman, A new fractional random wavelet transform for fingerprint security, *IEEE Trans. SMC*, Vol. 42, no. 1, pp. 262-275, 2012.

[5] A. Kanso and M. Ghebleh, A novel image encryption algorithm based on a 3D chaotic map, *Commun. Nonlinear Sci. Numer. Simul*, Vol. 17, no. 7, PP. 2943-2959, 2012.

[6] A.A. Abd El-Latif and X. Niu, A hybrid chaotic system and cyclic elliptic curve for image encryption, *AEU-Int. J. Electron. Commun*, Vol. 67, no. 2, pp. 136-143, 2013.

[7] C. Fu, B.B. Lin, Y.S. Miao, X. Liu, J.J. Chen, A novel chaos-based bit level permutation scheme for digital image encryption, *Opt. Commun*, Vol. 284, no. 23, pp. 5415-5423, 2011.

[8] A.A. Abd El-Latif, L .Li, N. Wang, Q. Han, X. Niu, A new approach to chaotic image encryption based on quantum chaotic system, exploiting color spaces, *Signal Process*, Vol. 93, no. 11, pp. 2986-3000, 2013.

[9] X. Wang and D. Luan, A novel image encryption algorithm using chaos and reversible cellular automata, Commun. Nonlinear Sci. Numer. Simul, Vol. 18, no. 11, pp. 3075-3085, 2013.

[10] C. Soutar and G. J. Tomko, Secure private key Generation using a Fingerprint, *Proc. CardTech/SecurTech Conf.*, Vol. 1, pp. 245-252, 1996.

[11] C. Soutar, D. Roberge, A. Stoianov, R. Gilroy, and B. V. K. V. Kumar, Biometrics encryption using image processing, *Proc. Of SPIE-Optical Security Counterfeit Deterrence Techniques II, San Jose, CA*, Vol. 3341, pp. 178-188, 1998.

[12] N. K. Ratha, J. Connell, and R. Bolle, Secure biometrics authentication, *Proc. Workshop Autom. Identification Adv. Technol., Morristown, NJ*, 1999.

[13] U. Uludag, S. Pankanti, and S. Prabhakar, Biometrics cryptosystems: Issues and challenges, *Proc. IEEE*, Vol. 92, no. 6, pp. 948-960, Jun. 2004.

[14] D. Moon, Y. Chung, S. B. Pan, K. Moon, and K. I. Chung, An efficient selective encryption of fingerprint images for embedded processors, *ETRIJ.* , Vol. 28, no. 4, pp. 444-452, Aug. 2006.

[15] N. Balaji and N. Nagaraj, Cryptanalysis of a chaotic image encryption algorithm, *National conference on nonlinear systems and dynamics*, Vol. 1, pp. 1-14, 2008.

[16] G. Bhatnagar, Q.M.J. Wu, Chaos-based security solution for fingerprint data during communication and transmission, *IEEE Trans.*, Vol. 61, no. 4, pp. 876-887, 2012.

[17] G. Bhatnagar and Q. M. Jonahtan Wu, A novel chaos-based secure transmission of biometric data, *Neurocomputing*, Vol. 147, no. 2, pp. 444-455, 2015.

[18] H. -I. Hsiao and J. Lee, Fingerprint image cryptography based on multiple chaotic systems, *Signal Process.*, Vol. 113, no. 4, pp. 169-181, 2015.

[19] M.A. Murillo-Escobar, C. Cruz-Hernndez, F. Abundiz-Prez, R.M. Lpez-Gutirrez, A robust embedded biometric authentication system based on fingerprint and chaotic encryption, *Expert Systems with Applications*, Vol.42 , no. 3, pp. 8198-8211, 2015.

[20] G. Bhatnagar, Q. M. J. Wu, Chaos-Based Security Solution for Fingerprint Data during Communication and Transmission, IEEE Trans. IM., Vol. 61, no. 4, APRIL 2012.

[21] R. Matthews, On the derivation of a chaotic encryption algorithm, *Cryptologia*, Vol. 13, no. 1, pp. 29-42, 1989.

[22] L. Kocarev, G. Jakimoski, T. Stojanovski, and U. Parlitz, From chaotic maps to encryption schemes, *IEEE Proc. Int. Symp. Circuits Syst.*, Vol. 4, pp. 514-517, 1998.

[23] G. Jakimoski and L. Kocarev, Chaos and cryptography: Block encryption ciphers based on chaotic maps, *IEEE Trans. Circuits Syst. I, Fundam. Theory Appl.*, Vol. 48, no. 2, pp. 163-169, Feb. 2001.

[24] F. Sun, S. Liu, Z. Li, and Z. Lu, A novel image encryption scheme based on spatial chaos map, *Chaos Solitons Fractals*, Vol. 38, no. 3, pp. 631-640, 2008.

[25] L. Zhang, X. Liao, and X. Wang, An image encryption approach based on chaotic maps, *Chaos Solitons Fractals*, Vol. 24, no. 3, pp. 759-765, 2005.

[26] N. K. Pareek, V. Patidar, and K. K. Sud, Image encryption using chaotic logistic map, *Image Vis. Comput.*, Vol. 24, no. 9, pp. 926-934, 2006.

[27] Z. J. Fang, X. Lu, W. M. Wei, and S. Z. Wang, mage scrambling based on bit shuffling of pixels, *J. Optoelectron. Laser*, Vol. 18, no. 12, pp. 1486-1488, 2007.

[28] T. G. Gao and Z. Q. Chen, Image encryption based on a new total shuffling algorithm, *Chaos Solitons Fractals*, Vol. 38, no. 1, pp. 213 220, 2008.

[29] F. Han, J. Hu, X. Yu, and Y. Wang Fingerprint images encryption via multi-scroll chaotic attractors, *Appl. Math. Comput*. Vol. 185, no. 2, pp. 931-939, 2007.

[30] S. Zhao, H. Li, and X. Yan, A secure and efficient fingerprint images encryption scheme, *Proc. Int. Conf. Young Comput. Sci.*, pp. 2803-2808, 2008.

[31] D. Cui, A novel fingerprint encryption algorithm based on chaotic system and fractional Fourier transform, *Proc. Int. Conf. Mach. Vis. Human-Machine Interface*, pp. 168-171, 2010.

[32] Y. Ruisong, G. Weichuang, A Chaos-based Image Encryption Scheme Using Multimodal Skew Tent Maps, *Journal of Emerging Trends in Computing and Information Sciences*, Vol. 4, No. 10, pp. 800-810, October 2013.

[33] H. Zhou, A design methodology of chaotic stream ciphers and the realization problems in finite precision, Ph.D. dissertation, Dept. Elect. Eng., Fudan Univ., Shanghai, China, 1996.

[34] http://en.pudn.com/downloads72/sourcecode/others/detail26410_en.html

[35] A. Sabri, Combinaison de la cryptographie et du watermarking pour renforcer la sécurité de la transmission des données biométriques dans un réseau informatique, thèse de magister, USTOMB-Alegria, 2013.

[36] Recommendation for Key Management: Part1: General (Revision3), NIST SP800-57, ⟨http://csrc.nist.gov/publications/nis tpubs/800-57/ sp800-57_part1_rev3_general.pdf⟩, 2012.

[37] H. Hsiao, J. Lee, Fingerprint image cryptography based on multiple chaotic systems, *Signal Processing*, Vol. 113, pp. 169–181, 2015.

[38] X. Wang, H. Zhang, A color image encryption with heterogeneous bit-permutation and correlated chaos, *Optics Communications*, Vol. 342, pp. 51–60, 2015.

[39] R. Liu, Chaos-based fingerprint images encryption using symmetric cryptography, *Proceedings of IEEE International Conference on Fuzzy Systems and Knowledge Discovery*, pp. 2153–2156, 2012.

[40] Y. Zhou, L. Bao, C.L. Philip Chen, Image encryption using a new parametric switching chaotic system, *Signal Process*,Vol. 93, no. 11, pp. 3039–3052, 2013.

[41] C. E. Shannon, Communication theory of secrecy system, Bell Syst. Tech. J, Vol. 28, pp. 656-715, 1949.

[42] S.M. Seyedzadeh, S. Mirzakuchaki, A fast color image encryption algorithm based on coupled two-dimensional piecewise chaotic map, *Signal Process*, Vol. 92, no. 5, pp. 1202-1215, 2012.

[43] C. Fu, J. Chen, H. Zou, W. Meng, Y. Zhan, Y. Yu, A chaos-based digital image encryption scheme with an improved diffusion strategy, *Opt. Express*, Vol. 20, no. 3,pp. 2363–2378, 2012.

[44] Y. Zhang, X. Wang, A symmetric image encryption algorithm based on mixed linear–nonlinear coupled map lattice, *Inf.Sci*. Vol. 273, pp. 329–351, 2014.

[45] Y. Wu, G. Yang, H. Jin, J.P. Noonan, Image encryption using the two-dimensional logistic chaotic map, *J. Electron. Imaging*, Vol. 21, no. 1, 2012.

[46] Y. Wu, Y. Zhou, G. Saveriades, S. Agaian, J.P. Noonan, P. Natarajan, Local Shannon entropy measure with statistical tests for image randomness, *Inf.Sci*. Vol. 222, pp. 323–342, 2013.

[47] F. Pareschi, R. Rovatti, G. Setti, On statistical tests for randomness included in the NISTSP800-22 Test Suite and based on the binomial distribution, *IEEE Trans. Inf. Forensics Secur*. Vol. 7, no. 2, pp. 491–505, 2012.

[48] A. SABRI, M. OUSLIM, Application of Chaotic Encryption to Secure the Fingerprint Data, International Review on Computers and Software, Vol. 11, N. 9, pp. 816-826, September 2016.

Efficient GeMSS Based Ring Signature Scheme

Murat Demircioglu
Institute of Applied Mathematics
Middle East Technical University
Ankara, Turkey
demircioglumurat@gmail.com

Sedat Akleylek*
Computer Engineering
Ondokuz Mayis University
Samsun, Turkey
sedat.akleylek@bil.omu.edu.tr

Murat Cenk
Institute of Applied Mathematics
Middle East Technical University
Ankara, Turkey
mcenk@metu.edu.tr

***Abstract*—The ring signature scheme has an important usage area of public key crypto-system. It can be used for e-voting, as well as leaking information without revealing identity within a group. However, most of these systems relies on traditional crypto-systems which are not secure against quantum computing related attacks. Multivariate cryptography is one of the most popular research area on quantum resilient crypto-systems. In this work, we propose an efficient ring signature scheme based on GeMSS, where we achieve smaller signature size and faster verification time with respect to other alternatives.**

***Index Terms*—post-quantum crptography, multivariate, GeMSS, ring signature**

I. Introduction

The security of modern public-key crypto-systems are mainly based on the difficulty of mathematical problems; such as integer factorization problem, discrete log problem, etc. However, these systems will become insecure as the large scale quantum computers are built. Shor's algorithm [1] solves these number theoretic problems on quantum computers in polynomial time. Therefore, there arises a need for alternative public-key systems that will be secure against quantum computer related attacks. This new area of study is called Post-Quantum Cryptography. Multivariate, lattice, isogeny, code and hash based crypto-systems are the candidates for it [2]. Among these, Multivariate crypto-systems are very fast and require modest computational power. Their security is based on *MQ Problem*. Although there exists many signature schemes such as Gui [3], Rainbow [4], and UOV [5], there is a lack of signature schemes with special properties such as ring signature, bling signature, threshold signature, etc.

In a ring signature scheme, a user in a group $\mathcal{R}$ is able to sign a message anonymously on behalf of the group, and nobody including the group members cannot reveal the true identity of the signer. This scheme can be used in leaking secrets, e-voting, electronic cash, etc. There are many ring signature schemes based on traditional public-key crypto-systems. The idea of the ring signature was firstly introduced by Rivest et al. [6], and they proposed the first ring signature scheme based on RSA algorithm. After that, a number of ring signature schemes that are based on multivariate cryptography have been proposed [7]–[10].

In this paper, we propose an efficient multivariate ring signature scheme that is based on GeMSS [11], which is one of the Round 2 candidates in Post-Quantum Standardization Call of NIST.

This paper is organized as follows. In Section II, we introduce the concept of ring signature scheme and multivariate crypto-system. A brief introduction to GeMSS is also given in this section. In Section III, we propose our ring signature algorithm. The public key and signature sizes, and the computation times of the proposed scheme are given in Section IV. We conclude the paper in Section V.

II. Preliminaries

A. Ring Signatures

In a group $\mathcal{R} = \{u_1, \ldots, u_t\}$ consisting of t-many possible signers, *Ring signature schemes* allow a member to sign a message anonymously on behalf of the group. The verifier can easily check if the message is signed by a member of the group. However, nobody including the group members can reveal the identity of the actual signer.

A ring signature scheme consists of three algorithms **KeyGen**, **RingSign**, and **Verify**.

- `Keygen(`1^λ`)` is a probabilistic algorithm that takes a security parameter λ as an input, and then generates a public and private key pair (sk, pk). By using this algorithm, each user $u_i \in \mathcal{R}$ generates their own key pairs to be used in a ring signature scheme.
- `RingSign(`$d,\ sk_i,\ \{pk_1, \ldots, pk_t\}$`)` is a probabilistic algorithm where the user $u_i \in \mathcal{R}$ signs the message d, and output is the signature σ.
- `Verify(`$(d, \sigma), \{pk_1, \ldots, pk_t\}$`)` is a deterministic algorithm that returns true only if the signature is valid.

A ring signature is assumed to be correct if the following equation holds

$$Pr[Verify((d, RingSign(d, sk_i, \{pk_1, \ldots, pk_t\})), \{pk_1, \ldots, pk_t\})] = 1 \quad (1)$$

for all $i \in \{1, \ldots, t\}$.

*Sedat Akleylek is partially supported by TUBITAK under grant no. EEEAG-116E279.

There are two basic security criteria for a ring signature scheme. These are anonymity and unforgeability.

- **Anonymity:** The verifier should not be able to find the actual signer of the given message.
- **Unforgeability:** An adversary not belonging to the group $\mathcal{R}$ should not be able to forge a valid signature on behalf of the group $\mathcal{R}$.

B. Multivariate Cryptography

The basic objects of multivariate cryptography are systems of multivariate quadratic polynomials in (2).

$$\begin{aligned} f^{(1)}(x_1,\ldots,x_n) &= \sum_{i=1}^{n}\sum_{j=1}^{n} f_{ij}^{(1)}\cdot x_i x_j + \sum_{i=1}^{n} f_i^{(1)}\cdot x_i + f_0^{(1)} \\ f^{(2)}(x_1,\ldots,x_n) &= \sum_{i=1}^{n}\sum_{j=1}^{n} f_{ij}^{(2)}\cdot x_i x_j + \sum_{i=1}^{n} f_i^{(2)}\cdot x_i + f_0^{(2)} \\ &\vdots \\ f^{(m)}(x_1,\ldots,x_n) &= \sum_{i=1}^{n}\sum_{j=1}^{n} f_{ij}^{(m)}\cdot x_i x_j + \sum_{i=1}^{n} f_i^{(m)}\cdot x_i + f_0^{(m)} \end{aligned} \tag{2}$$

Let $\mathbb{F}$ be a finite field. The main idea is to choose the central map $\mathcal{F}:\mathbb{F}^m\to\mathbb{F}^n$, which is a multivariate system of easily invertible quadratic polynomials. After the choice of $\mathcal{F}$, two affine linear invertible maps $\mathcal{S}:\mathbb{F}^m\to\mathbb{F}^m$ and $\mathcal{T}:\mathbb{F}^n\to\mathbb{F}^n$ are chosen to hide the structure of the central map. Therefore, public-key is $\mathcal{P}=\mathcal{S}\circ\mathcal{F}\circ\mathcal{T}:\mathbb{F}^n\to\mathbb{F}^m$, and private key is $(\mathcal{S},\mathcal{F},\mathcal{T})$.

The security is based on the **MQ Problem:** Given m multivariate quadratic polynomials $f^{(1)}(x),\ldots,f^{(m)}(x)$ in n variables $x_1,\ldots,x_n$ as stated in (2), find a vector $\overline{x}=(x_1,\ldots,x_n)$ such that $f^{(1)}(\overline{x})=\cdots=f^{(m)}(\overline{x})=0$. The MQ problem (for $m\approx n$) is proven to be NP-hard even for quadratic polynomials over $\mathbb{F}_2$ [12].

The generic multivariate signature scheme consists of:

- **Signature Generation:** In order to sign a message M, the signer uses a hash function $\mathcal{H}:\{0,1\}\to\mathbb{F}^m$ to compute $h=\mathcal{H}(M)\in\mathbb{F}^m$. Then he calculates computes recursively $x=\mathcal{S}^{-1}(h)\in\mathbb{F}^m$, $y=\mathcal{F}^{-1}(x)\in\mathbb{F}^n$ and $z=\mathcal{S}^{-1}(y)\in\mathbb{F}^n$. At the end, the signature of the message M is $\sigma=\mathcal{T}^{-1}(\mathcal{F}^{-1}(\mathcal{S}^{-1}(h)))$.
- **Signature Verification:** In order to check if the signature σ is valid for the message M, the verifies computes $h=\mathcal{H}(M)$ and $h'=\mathcal{P}(\sigma)$. If they are same, then the signature is valid, otherwise not.

C. GeMSS

GeMSS [11] (Great Multivariate Short Signature) is a multivariate-based signature scheme with small signature size, fast verification process and medium/large public-key size. It is one of the Round 2 candidates in the NIST's Post-Quantum Cryptography Standardization. As well as being in direct lineage from QUARTZ [13], GeMSS borrows some design rationale of the Gui multivariate signature scheme [14].

The main parameters of GeMSS are:

- D, a positive integer that is the degree of a secret polynomial,
- K, the output size in bits of the hash function,
- λ, the security level of GeMSS,
- m, number of equation in the public-key,
- $nb\_ite>1$, number of iterations in the public-key,
- n, the degree of a field extension,
- v, the number of vinegar variables,
- Δ, the number of minus, where $m=n-\Delta$.

The **public-key** in GeMSS is a set $\mathcal{P}=(f_1,\ldots,f_m)\in\mathbb{F}_2[x_1,\ldots,x_{n+v}]^m$ of m quadratic equations in $n+v$ variables. The **secret-key** is composed of a couple of invertible matrices $(\mathcal{S},\mathcal{T})\in\mathsf{GL}_{n+v}(\mathbb{F}_2)\times\mathsf{GL}_n(\mathbb{F}_2)$ and a polynomial $\mathcal{F}\in\mathbb{F}_{2^n}[X,v_1,\ldots,v_v]$.

There are three main algorithms of GeMSS; key generation, signing and verification processes. Let $\mathbb{F}=\mathbb{F}_2$ and choose $nb\_ite=4$ as in QUARTZ [13].

1) Let *GKeyGen* be the function to generate GeMSS keypair (pk,sk).
   - **Input:** GeMSS parameters (λ,D,n,v,m)
   - **Output:** GeMSS keypair $(sk,pk)=((\mathcal{S},\mathcal{F},\mathcal{T}),\mathcal{P})$
2) Let *GSign* be the function to generate a GeMSS signature σ for a given message M.
   - **Input:** GeMSS private-key $sk=(\mathcal{S},\mathcal{F},\mathcal{T})$, message M, repetition factor nb_ite
   - **Output:** Signature $\sigma=(S_{nb\_ite},X_{nb\_ite},\ldots,X_1)\in\mathbb{F}^{m+nb\_ite(n+v-m)}$
3) Let *GVer* be the function to verify if the given GeMSS signature is valid.
   - **Input:** Signature σ, GeMSS public key pk, message M, repetition factor nb_ite
   - **Output:** $S_0\in\mathbb{F}^m$. If it is equal to zero, then the signature is valid. Otherwise, it is not valid.

III. GeMSS Based Ring Signature Scheme

In this section, we propose a new multivariate ring signature scheme based on GeMSS signature algorithm. Since the propose scheme is mainly based on the verification algorithm, GeMSS is a perfect choice with its fast verification time and small signature size.

Let $\mathcal{R}=\{u_1,\ldots,u_t\}$ be a group of t users.

Key Generation: Each user $u_i\in\mathcal{R}$ generates a key pair $(sk_i,pk_i)=((\mathcal{S}_i,\mathcal{F}_i,\mathcal{T}_i),\mathcal{P}_i)$ by using the key generation function *GKeyGen* of GeMSS, where

$$\begin{aligned} (\mathcal{S}_i,\mathcal{T}_i) &\in \mathsf{GL}_{n+v}(\mathbb{F}_2)\times\mathsf{GL}_n(\mathbb{F}_2) \\ \mathcal{F}_i &\in \mathbb{F}_{2^n}[X,v_1,\ldots,v_v] \\ \mathcal{P}_i &\in \mathbb{F}_2[x_1,\ldots,x_{n+v}]^m \end{aligned} \tag{3}$$

The group public key is the concatenation of the public keys of all users, i.e. $\mathcal{P} = \mathcal{P}_1 \| \mathcal{P}_2 \| \cdots \| \mathcal{P}_t$. Each user u_i keeps their private key $sk_i = (\mathcal{S}_i, \mathcal{F}_i, \mathcal{T}_i)$ as secret.

Signature Generation: In order to sign a message M on behalf of the group $\mathcal{R}$, a user u_i should follow the following steps:

1) Compute the hash of the message M and take first m-bits:
$$h = \mathcal{H} \in \mathbb{F}_2^m \tag{4}$$
2) Choose random vectors $\sigma_1, \ldots, \sigma_{i-1}, \sigma_{i+1}, \ldots, \sigma_t \in \mathbb{F}_2^{m+nb\_ite(n+v-m)}$, and then compute
$$\overline{h} = h - \sum_{j=1, j\neq i}^{t} GVer(\sigma_j, pk_j, M, nb\_ite) \tag{5}$$
3) Use private key sk_i to compute a vector σ_i such that $GVer(\sigma_i, pk_i, M, nb\_ite) = \overline{h}$

The ring signature for the message M is $\sigma = (\sigma_1, \ldots, \sigma_t) \in \mathbb{F}_2^{[m+nb\_ite(n+v-m)]t}$

Signature Verification: In order to check if the given signature σ is valid for the message M, the verifier follows the following steps:

1) Compute the hash of the message M and take first m-bits:
$$h = \mathcal{H} \in \mathbb{F}_2^m \tag{6}$$
2) Use the group public key and compute
$$\overline{h} = \sum_{j=1}^{t} GVer(\sigma_j, pk_j, M, nb\_ite) \tag{7}$$

If $\overline{h} = h$ holds, then the signature is valid. Otherwise, the given signature for the message M is not valid.

IV. Performance Analysis

Table I shows the parameters for different security levels of GeMSS that are given in ([11], Section 3).

TABLE I
PERFORMANCE ANALYSIS OF GEMSS

	pk size (kB)	sign. size (bit)	sign (ms)	verify (ms)
GeMSS128	352.18	258	260	0.041
GeMSS192	1,237.960	411	694	0.117
GeMSS256	3,040.690	576	1,090	0.336

We use this table to calculate the signature size and approximate calculation time of our proposed ring signature scheme. Size of the group public key $\mathcal{P}$ can be calculated by simply multiplying the number of group members with the size of a public key for the chosen security level. In order to calculate the size of the ring signature, we sum up m-bits from the hash of the message, size of the nb_ite (which is taken constant 4 $\approx$ 3-bits), and t-many size of signatures where t is the number of grup members. In order to sign a message on behalf of the grup, a user u_i will perform $t-1$ evaluations of *GVer*, and 1 evaluation of *GSign* functions. The verification can be done by t evaluations of *GVer* function.

V. Conclusion

GeMSS, GUI and Rainbow algorithms are multivariate based cryptosystems that are proposed in the NIST's competition. If we compare the size of their key and signature, and performance on their reference implementation results under the same security levels, one can see that the GeMSS and GUI provides smaller signature sizes and faster verification times with respect to Rainbow. If we compare GeMSS and GUI, we will find that GeMSS provide smaller public key and signature sizes, and much more faster verification time.Furthermore, as the security level increases, GeMSS achieves faster signature generation time. Since our ring signature scheme mainly based on signature verification algorithm as stated above, using GeMSS as a signature algorithm in a ring signature scheme will result in a faster evaluation time and smaller signature sizes with respect to the ring signature schemes [15] and [16] that are based on GUI and Rainbow, respectively.

References

[1] Peter W. Shor, "Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer", SIAM Review 41(2): 303-332 (1999).

[2] D.J. Bernstein, J. Buchmann, E. Dahmen (eds.): "Post Quantum Cryptography", Springer, 2009 Berlin: Springer-Verlag, 2002, 533–547

[3] A. Petzoldt, M.S. Chen, B.Y. Yang, C. Tao, J. Ding: "Design Principles for HFEv- based Signature Schemes", ASIACRYPT 2015 - Part 1, LNCS vol. 9452, pp. 311-334. Springer, 2015.

[4] J. Ding, D. S. Schmidt: "Rainbow, a new multivariate polynomial signature scheme", ACNS 2005, LNCS vol. 3531, pp. 164-175. Springer, 2005.

[5] A. Kipnis, L. Patarin, L. Goubin: "Unbalanced Oil and Vinegar Schemes", EUROCRYPT 1999, LNCS vol. 1592, pp. 206-222. Springer, 1999.

[6] R.L. Rivest, A. Shamir, Y. Tauman, "How to Leak a Secret", in: Cryptology–Asiacrypt 2001, in: LNCS, vol. 2248, Springer-Verlag, Berlin, 2001, pp. 552–565.

[7] A. Petzoldt, S. Bulygin, J. Buchmann: "A Multivariate Threshold Ring Signature Scheme", AAECC 25 (3-4), pp. 255 - 275 (2012).

[8] S. Wang, R. Ma, Y. Zhang, X. Wang: "Ring signature scheme based on multivariate public key cryptosystems", Computers and Mathematics with Applications 62 (2011) 3973-3979.

[9] L.L. Wang: "A New Multivariate-based Ring Signature Scheme", Proceedings of ISCCCA 2013.

[10] J. Zhang, Y. Zhao: "A New Multivariate Based Threshold Ring Signature Scheme", NSS 14, LNCS vol. 8792, pp. 526 - 533. Springer 2014.

[11] Casanova, Antoine and Faugère, Jean-Charles and Macario-Rat, Gilles and Patarin, Jacques and Perret, Ludovic and Ryckeghem, Jocelyn, "GeMSS: A Great Multivariate Short Signature",Research Report, https://hal.inria.fr/hal-01662158, 2017

[12] M. R. Garey and D. S. Johnson: "Computers and Intractability: A Guide to the Theory of NP-Completeness", W.H. Freeman and Company 1979.

[13] J. Patarin, N. Courtois, and L. Goubin. "Quartz, 128-bit long digital signatures", In David Naccache, editor, Topics in Cryptology - CT-RSA 2001, The Cryptographer's Track at RSA Conference 2001, San Francisco, CA, USA, April 8-12, 2001, Proceedings, volume 2020 of Lecture Notes in Computer Science, pages 282-297. Springer, 2001.

[14] J. Ding and B. Yang. "Degree of regularity for HFEv and HFEv-", In Philippe Gaborit, editor, Post-Quantum Cryptography - 5th International Workshop, PQCrypto 2013, Limoges, France, June 4-7, 2013. Proceedings, volume 7932 of Lecture Notes in Computer Science, pages 52-66. Springer, 2013.

[15] S. Akleylek, M. Demircioglu, and M. Cenk, “GUI Based Ring Signature Scheme,” presented at the 18th Central European Conference on Cryptology (CECC 2018), Smolenice, 2018.
[16] M. S. E. Mohamed, A. Petzoldt, ”RingRainbow – An Efficient Multivariate Ring Signature Scheme”. AFRICACRYPT 2017, LNCS vol.10239, pages 3-20. Springer, 2017.

A Different Encryption System Based on the Integer Factorization Problem

Karima Djebaili, Lamine Melkemi

Department of Computer Science and Information Technologies, University of Ouargla, Ouargla, Algeria
djebaili.karima@univ-ouargla.dz
Department of Mathematics, University of Batna, Batna, Algeria
lamine.melkemi@univ-batna

Abstract

We present a new computational problem in this paper, namely the order of a group element problem which is based on the factorization problem, and we analyze its applications in cryptography.We present a new one-way function and from this function we propose a homomorphic probabilistic scheme for encryption. Our scheme, provably secure under the new computational problem in the standard model.

Keywords: *Public key encryption, factorization problem, order of a group element problem.*

1 Background

The idea of public-key encryption was introduced by Diffie and Hellman (1976) Several cryptographic schemes take place in the multiplicative group $\mathbb{Z}_n^*$, under the assumption that it is difficult to invert the one-way function of an encryption process without the knowledge of the factorization of the composite number $n = pq$ where p and q are two large prime numbers. Real examples of such schemes [Rivest et al. (1978),Rabin (1979),Cohen and Fischer (1985),Kurosawa et al. (1991),Paillier (1999)] and digital signatures [Cramer and Shoup (2000),Camenisch and Lysyanskaya (2003). In this paper we propose two schemes; public key encryption scheme and a signature scheme and we will demonstrate their security under the order of a group element problem which is based on the factorization problem.

2 Notations

Consider an RSA-modulus $n = pq$, where p and q are large primes. Assume that $x \in \mathbb{Z}_n^*$, the order of x is defined to be the least positive integer z such that $x^z = 1 \mod n$, (see Menezes et al. (1996)). In our case such an integer z ($x^z = 1 \mod n$) always exists. We denote by $|x|$ the order of x. Moreover the subgroup generated by x denoted by $< x >$.
It is well known that the order $|x|$ of x divides the Euler totient function $\phi(n) = (p-1)(q-1)$.

2.1 Key Generation and Cryptographic Scheme

Depending on the security parameter, a one-way function defines the public and secret keys of a public key encryption (PKE) scheme for each user: a $\mathcal{G}$ key generation algorithm takes as argument the security parameter k, then randomly sets public key pk and secret key sk: $(pk, sk) \leftarrow \mathcal{G}(1^k)$. We denote m and c for the message and ciphertext respectively.

2.2 The Order of a Group Element Problem

Let x be an element in $\mathbb{Z}_n^*$. Given $x^z = 1 \bmod n$, the Assumption 1 define the order of a group element problem as the computational problem of computing z. We assume this problem is difficult without the knowledge of factorization of the modulus n.

Assumption 1 *(**The order of a group element problem**). For every probabilistic polynomial time (PPT) adversary $\mathcal{A}$, there exists a negligible function $negl(.)$ and a security parameter k_0 such that the following holds for all $k > k_0$:*

$$Pr[z \leftarrow \mathcal{A}(x, \mathbb{Z}_n^*) | x^z = 1 \; mod \, n] = negl(k). \tag{1}$$

2.3 Semantic security

Semantic security (see Goldwasser and Micali (1984)) also known as indistinguishability of ciphertexts or polynomial security, it is like *perfect security* but we only allow an adversary with polynomially bounded computing power.

Definition 1 *(**Semantic security**). A PKE scheme is said to be semantically secure (or IND-CPA secure) if for any adversary $\mathcal{A}$ uses a pair of PPT algorithms $(\mathcal{A}_1, \mathcal{A}_2)$ the following advantage Adv holds for $n, k \in \mathbb{N}$ and some state information:*

$$\begin{aligned} Adv_{\mathcal{A}}^{IND-CPA} = Pr[b \leftarrow \mathcal{A}_2(c, state) | (pk, sk) \leftarrow \mathcal{G}(1^k), (m_0, m_1, state) \leftarrow \mathcal{A}_1, \\ c \leftarrow Encrypt(m_b, pk)] < \frac{1}{2} + \frac{1}{n^k}. \end{aligned} \tag{2}$$

3 Encrypting Protocol

This section describes the encryption scheme proposed in this paper which consists of three algorithms:

- **Key generation**: Select an RSA-modulus $n = pq$ where p and q are co-prime and select $\alpha, \beta \in \mathbb{Z}_n^*$ where $\alpha = \frac{p-1}{2}$ and $\beta = \frac{q-1}{2}$, that is $\delta\alpha + \gamma\beta = 1$ for two integers δ and γ. Now select a and b such that $|a| = \alpha$ and $|b| = \beta$. The public key $pk = (n, a, b)$ and the secret key $sk = (p, q, \delta, \gamma)$. Each public key is associated with a message space $MsgSp(pk)$ and a ciphertext space $CipSp(pk)$.
- **Encryption**: We wish to encrypt a message $m \in MsgSp(pk)$. The ciphertext is $c_1 = a^x m \bmod n$ and $c_2 = b^y m \bmod n$, for two random values x and $y \in \mathbb{Z}_n$.

- **Decryption**: Given a ciphertext $(c_1, c_2) \in CipSp(pk)$ we output $m = c_1^{\delta\alpha} c_2^{\gamma\beta} \bmod n$.

3.0.1 Proof of Decryption Validity

At the time of decryption the receiver computes:

$$\begin{aligned} c_1^{\delta\alpha} c_2^{\gamma\beta} \bmod n &= (a^x)^{\delta\alpha} m^{\delta\alpha} (b^y)^{\gamma\beta} m^{\gamma\beta} \bmod n \\ &= (a^\alpha)^{\delta x} m^{\delta\alpha} (b^\beta)^{\gamma y} m^{\gamma\beta} \bmod n \\ &= m^{\delta\alpha} m^{\gamma\beta} \bmod n \\ &= m^{\delta\alpha+\gamma\beta} \bmod n \\ &= m \bmod n \\ &= m. \end{aligned} \tag{3}$$

3.1 Security Analysis

This section discusses the security results of the cryptosystem proposed in this paper.

3.1.1 One-Wayness

Theorem 1 *The proposed encryption function provides one-wayness if there is no adversary who can recover p and q.*

Proof. It is easy to see that if the problem of factorization is not intractable in $\mathbb{Z}_n^*$, it is easy to recover the secret key (i.e, α and β), from which the determination of m is obvious. □

3.1.2 IND-CPA Security

Definition 2 ***(Decisional generator problem)****.Select an RSA-modulus $n = pq$. Define the formulation:*

$$a, b, f, g \in \mathbb{Z}_n^* \text{ determine if } f \in < a > \text{ and } g \in < b > .$$

We call this the decisional generator problem (DGP) which is based on the integer factorization problem.

A) **The Proposed Cryptosystem is at Least as Hard as The DGP**

Theorem 2 *If the proposed cryptosystem is not secure in the sense of IND-CPA attacks, then there is an adversary that solves the DGP with non-negligible advantage.*

Proof. Assume that $\mathcal{A}$ is an adversary that can break the proposed cryptosystem in the sense of IND-CPA with a non-negligible advantage ϵ, we will use

this to create a new adversary $\mathcal{B}$ which breaks the DGP. The following discussion describes the construction of $\mathcal{B}$:

Algorithm $\mathcal{B}$:
The algorithm is given $\mathbb{Z}_n^*, a, b, f, g$ as input.

- Set $pk = (n, a, b)$ and run $\mathcal{A}(pk)$ to obtain two messages m_0,m_1.
- Choose a random bit $b \in \{0, 1\}$, and set:
  (a) $c_1 = fm_b \bmod n$.
  (b) $c_2 = gm_b \bmod n$.
- Give the ciphertext (c_1, c_2) to $\mathcal{A}$ and obtain an output bit b'.
  If $b' = b$ output 1; otherwise output 0.

We analyze the behavior of $\mathcal{B}$. There are two cases.

Case 1. If $f \in < a >$ and $g \in < b >$ then (c_1, c_2) is a valid encryption, so $\mathcal{A}$ will guess correctly b with non-negligible probability, therefore:

$$Pr[\mathcal{B} \text{ output=1}] = \frac{1}{2} + \epsilon.$$

Case 2. If f and g are random numbers then in this case, b is independent of the adversary's view, therefore:

$$Pr[\mathcal{B} \text{ output=0}] = \frac{1}{2}.$$

B) **The DGP is at Least as Hard as the Proposed Cryptosystem**

Theorem 3 *If there exists an oracle O which solves the DGP with non-negligible probability, then the proposed cryptosystem is not secure in the sense of IND-CPA.*

Proof. We assume that we have an oracle O which solves the DGP such that solving this problem permits the adversary $\mathcal{A}$ to distinguish the ciphertext for messages m_0 and m_1. If f (or g) (ff and g are the input of this oracle), $\in < a >$ (or $\in < b >$), O outputs 1; otherwise it output 0. $\mathcal{A}$ should run in two stages:

- **Find stage:** At this stage $\mathcal{A}$ asked the encryption oracle on two messages m_0, m_1, such that $gcd(m_0, \phi) = 1$, the outputs of this oracle is:

$$[fm_i, gm_i], [fm_{1-i}, gm_{1-i}] \text{ where } i \in \{0, 1\}.$$

- **Guess stage:** At this stage $\mathcal{A}$ asked the oracle O on:

$$[fm_i m_0^{-1}, gm_i m_0^{-1}].$$

If the output of the oracle O is 1 (i.e.,$f \in < a >$ or $g \in < b >$) with probability non-negligibly, then $m_i = m_0$. Otherwise $m_i = m_1$.

Because the hardness assumption of the integer factorization problem it is difficult to find α and β, so the probability of determine whether or not $f \in < a >$ and $g \in < b >$ is negligible, which means that the proposed cryptosystem is IND-CPA secure and this concludes the proof. □

4 Signing Protocol

Let m be a message which the sender wishes to sign. He performs the following singing protocol which consists of three algorithms.

- **Key generation:** Select an RSA-modulus $n = pq$ where p and q are co-prime and select $\alpha, \beta \in \mathbb{Z}_n^*$ where $\alpha = \frac{p-1}{2}$ and $\beta = \frac{q-1}{2}$, that is $\delta\alpha + \gamma\beta = 1$ for two integers δ and γ. Now select a and b such that $|a| = \alpha$ and $|b| = \beta$. Public verification key $vk = (n, a, b)$. Private signature key $sk = (p, q, \delta, \gamma)$. Each public verification key is associated with a message space $MsgSp(vk)$ and a signing-message space $SigSp(vk)$.

- **Signature:** To sign a message $m \in MsgSp(vk)$, Choose at random $\varphi \in < a >$ and $\psi \in < b >$. Compute $c_1 = (\varphi h(m))^\beta \bmod n$, $c_2 = (\psi h(m))^\alpha \bmod n$ and $\omega = (\varphi\psi)^{-1} \bmod n$, where $h(.)$ is a cryptographic hash function. The signature on m is $(c_1, c_2, \omega) \in SigSp(vk)$.

- **Verification:** Given a signature (c_1, c_2, ω) on $m \in MsgSp(vk)$. Accept if $h(m) = c_1^\gamma c_2^\delta \omega \bmod n$.

4.1 Proof of Verification Validity

At the time of verification the receiver computes:

$$\begin{aligned} c_1^\gamma c_2^\delta \bmod n &= \varphi^{\gamma\beta} h(m)^{\gamma\beta} \psi^{\delta\alpha} h(m)^{\delta\alpha} \bmod n \\ &= \varphi^{\gamma\beta} \psi^{\delta\alpha} h(m)^{\delta\alpha+\gamma\beta} \bmod n \\ &= \varphi^{\gamma\beta} \psi^{\delta\alpha} h(m) \bmod n. \end{aligned} \tag{4}$$

and because:

$$\begin{aligned} \varphi\psi \bmod n &= (\varphi\psi)^{\delta\alpha+\gamma\beta} \bmod n \\ &= \varphi^{\delta\alpha+\gamma\beta} \psi^{\delta\alpha+\gamma\beta} \bmod n \\ &= \varphi^{\gamma\beta} \psi^{\delta\alpha} \bmod n. \end{aligned} \tag{5}$$

From 4 and 5, he finds $h(m) = c_1^\gamma c_2^\delta \omega \mod \text{n}$, so the verification condition holds.

4.2 Security Analysis

An adversary might attempt to forge user's signature on m by selecting a random integers $\varphi \in< a >$ and $\psi \in< b >$. The adversary must then determine $c_1 = (\varphi h(m))^{\beta} \bmod n$ and $c_2 = (\psi h(m))^{\alpha} \bmod n$. If the order of a group element problem is computationally infeasible in $\mathbb{Z}_n^*$, the adversary can do no better than to choose a c_1 and c_2 at random, this forgery only occurs with negligible probability.

5 Conclusions and Further Research

We constructed two systems that are provably secure under the order of a group element problem which is based on the factorization problem. The first construction is a public key cryptosystem and the second construction is a signature scheme. As future work we look to improve our main schemes to ensure security in the sense of NM-CCA2 (see Djebaili and Melkemi (2018)). However, these schemes are quite practical and more efficient compared with other schemes.

References

Camenisch, J. and A. Lysyanskaya (2003). A signature scheme with efficient protocols. In *Security in communication networks*, pp. 268–289. Springer.

Cohen, J. D. and M. J. Fischer (1985). *A robust and verifiable cryptographically secure election scheme*. Yale University. Department of Computer Science.

Cramer, R. and V. Shoup (2000). Signature schemes based on the strong rsa assumption. *ACM Transactions on Information and System Security (TISSEC) 3*(3), 161–185.

Diffie, W. and M. E. Hellman (1976). New directions in cryptography. *Information Theory, IEEE Transactions on 22*(6), 644–654.

Djebaili, K. and L. Melkemi (2018). Security and robustness of a modified elgamal encryption scheme. *International Journal of Information and Communication Technology 13*(3), 375–387.

Goldwasser, S. and S. Micali (1984). Probabilistic encryption. *Journal of computer and system sciences 28*(2), 270–299.

Kurosawa, K., Y. Katayama, W. Ogata, and S. Tsujii (1991). General public key residue cryptosystems and mental poker protocols. In *Advances in Cryptology-EUROCRYPT'90*, pp. 374–388. Springer.

Menezes, A. J., P. C. Van Oorschot, and S. A. Vanstone (1996). *Handbook of applied cryptography*. CRC press.

Paillier, P. (1999). Public-key cryptosystems based on composite degree residuosity classes. In *Advances in cryptology-EUROCRYPT'99*, pp. 223–238. Springer.

Rabin, M. O. (1979). Digitalized signatures and public-key functions as intractable as factorization.

Rivest, R. L., A. Shamir, and L. Adleman (1978). A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM 21*(2), 120–126.

Lifted Codes over Finite Chain Rings

1st Reguia Lamia Bouzara
Faculty of mathematics
University of Science and Technology Houari Boumediene
Algiers, Algeria
bouzaralamia@outlook.fr

2nd Edgar Martinez-Moro
Institute of Mathematics
University of Valladolid
Valladolid, Spain
Edgar.Martinez@uva.es

3rd Kenza Guenda
Faculty of mathematics
University of Science and Technology Houari Boumediene
Algiers, Algeria
ken.guenda@gmail.com

***Abstract*—In this paper we give the generalization of lifted codes over any finite chain ring. This has been done by using the construction of finite chain rings from p-adic fields.**

***Index Terms*—valuation rings, finite chain rings, lifted codes.**

I. Introduction

Finite commutative chain rings are finite local rings whose maximal ideals are principal, they can also be constructed from p-adic fields [4]. Let K be a finite extension of the field of p-adic numbers $\mathbb{Q}_p$ with residue degree r and ramification index s, let $\mathcal{O}_K$ be the ring of integers of K and π be a prime of K. Then $\mathcal{O}_K/\pi^{(n-1)s+t}$ is a finite commutatice chain ring of invariants (p, n, r, s, t) and every finite commutative chain ring can be obtained in this way.

Codes over finite rings have received a good deal of attention, due to the interesting results that have been obtained from studying this codes and there relationship with lattices construction. p-adic codes were studied in [1] where Calderbank and Sloane investigated codes over p-adic integers and studied lifts of codes over $\mathbb{F}_p$ and $\mathbb{Z}_{p^e}$ and to the p-adic integers. Lifted codes over finite chain rings were studied in [2], however the study is restricted to the finite chain rings of the form $\mathbb{F}_q[t]/\langle t^k\rangle$. Dougehrty used codes over p-adic integers to lift codes over finite chain rings and study this codes in this concept.

In this paper we propose to investigate the definition of finite chain rings as non-trivial quotient of ring integers of p-adic fields to give a general and a unified treatment valid for all finite chain rings.

II. Preliminaries

We refer the reader to [6] and [9] for the proofs of this section.

Let p be a prime number, and let x be an element of the rational field $\mathbb{Q}$, then x can be written in a unique way; $x = p^a\frac{m}{n}$, where $m \in \mathbb{Z}^*$ and $n \in \mathbb{N}^*$ such that m and n are not divisible by p. We define the p-adic valuation and the p-adic valuation of x as follow:

Definition .1: The p-adic valuation on the rational field $\mathbb{Q}$ is defined as:

$$v_p(0) = +\infty \ ; \ v_p(x) = a, \ \textit{where } x = p^a\frac{m}{n}.$$

Definition .2: The p-adic norm is an ulrametric absolute value given by

$$|x|_p = p^{-v_p(x)}.$$

Definition .3: The completion of $\mathbb{Q}$ by $|\cdot|$ is the field of p-adic numbers and we denote it by $\mathbb{Q}_p$.

The next proposition charactrise the field $\mathbb{Q}_p$

Proposition .1: Let $\mathbb{Q}_p$ be the field of p-adic numbers.

- The set $\mathbb{Z}_p = \{a \in \mathbb{Q}_p \ ; \ v(a) \geqslant 0\} = \{a \in \mathbb{Q}_p \ ; \ |a| \leqslant 1\}$. is a unitary subring of $\mathbb{Z}_p$ called the valuation ring or the ring of integers of $\mathbb{Q}_p$.
- $\mathbb{Q}_p = \mathcal{F}(\mathbb{Z}_p)$ where $\mathcal{F}(\mathbb{Z}_p)$ is the field of fractions of $\mathbb{Z}_p$.
- $\mathfrak{m} = \{a \in \mathbb{Q}_p \ ; \ v(a) > 0\} = \{a \in \mathbb{Q}_p \ ; \ |a| < 1\}$, is the unique maximal ideal of $\mathbb{Z}_p$, and it is generated by p and we write $\mathfrak{m} = \langle p\rangle$.
  $\mathfrak{m}$ is called ideal of the valuation v, and $\mathbb{Z}_p$ is a local ring.
- The quotient ring $k = \mathbb{Z}_p/\mathfrak{m} = \mathbb{F}_p$ is a field called residual field of the valuation v.
- Let $a \in \mathbb{Z}_p$ then we can write a as follow:

$$a = \sum_{i=0}^{+\infty} a_i p^i \ ; \ a_i \in \mathbb{F}_p.$$

A. Finite algebraic extension of $\mathbb{Q}_p$:

Let K be a finite algebraic extension of $\mathbb{Q}_p$ of degree n. Let $x \in K$, we denote $N_{K/\mathbb{Q}_p}(x)$ the endomorphism determinant of the $\mathbb{Q}_p$-vector space K defined by the multiplication by x. the characteristic polynomial of this endomorphism is:

$$X^n + ... + (-1)^n N(x)$$

is annulled by x in K. It is equivalent to say that x is un integer of K (ie. an element of B) or its normal polynomial is coefficient in $\mathbb{Z}_p$. We have also $\mathbb{Z}_p = \mathcal{O}_K \cap \mathbb{Q}_p$ we call also

the integer of $\mathbb{Q}_p$ the element of $\mathbb{Z}_p$. The next proposition define the valuation of K.

Proposition .2: Let K be an extension of $\mathbb{Q}_p$ of degree n, the relation:

$$w(x) = 1/nv(N_{L/K}(x))$$

define the unique valuation w of K extending the valuation v of $\mathbb{Q}_p$

Let u be the restriction of the valuation w over $\mathbb{Q}_p$ then we define the ramification index as follow

Definition .4: The ramification index of K is defined by

$$e = [w(K^*) : v(\mathbb{Q}_p^*)]$$

or simply we can define $e = w(p)$.

Proposition .3: Let K

- the ring of integers of K is denoted by $\mathcal{O}_K$ such that
$$\mathcal{O}_K = \{a \in \mathbb{Q}_p \ ; \ w(a) \geqslant 0\}$$
- let $\mathfrak{m}_K$ be the maximal ideal of $\mathcal{O}_K$, and let π be in $\mathfrak{m}_K$ but not in $\mathfrak{m}_K^2$ such that $w(\pi) = 1$ then we say that π is an uniformizer of $\mathcal{O}_K$.
- The maximal ideal of the ring $\mathcal{O}_K$ is generated by the uniformizer π and we write $\mathfrak{m}_K = \langle \pi \rangle$.
- $\mathcal{O}_K/\mathfrak{m}_K = \mathbb{F}_{p^f}$ we say that f is the inertial degree.
- Let p be a uniformizer of $\mathbb{Q}_p$ and π a uniformizer of K. Then
$$|p|_p = |\pi|_p^e$$
where e is the ramification index.
- $[K : \mathbb{Q}_p] = n = ef$
- Let α be an element of $\mathcal{O}_K$ then α can be written as follow
$$\alpha = \sum_{i=0}^{+\infty} a_i \pi^i;$$
where a_i are element of $\mathcal{O}_K/\mathfrak{m}_K = \mathbb{F}_{p^f}$.

The next theorem is a local version of the fact that if K is a number field, then $\mathcal{O}_K$ is a free $\mathbb{Z}_p$-module of rank $[K : \mathbb{Q}_p]$.

Theorem .1: Let K be a finite extension of $\mathbb{Q}_p$ of degree n, then we have that the $\mathbb{Z}_p$-module $\mathcal{O}_K$ is free of rank

$$n = [K : \mathbb{Q}_p] = ef.$$

such that if $\{\alpha_1, ..., \alpha_f\} \subset \mathbb{Z}_p$ is a set such that the reductions $\overline{\alpha}_i$ generates $\mathbb{F}_{p^f}$ as an $\mathbb{F}_p-$vector space, the the set

$$\{\alpha_j \pi_K^k\}_{0 \leq k \leq e, 1 \leq j \leq f}$$

is an $\mathbb{Z}_p$-basis of $\mathcal{O}_K$.

III. Finite Chain Rings and Lifted Codes

Finite commutative chain rings are finite rings whose ideals form a chain under unclusion. Let R be a finite chain ring of characteristic p^n with maxiaml ideal M and nilpotency index s, the quotient R/M is a field called residue field of R with characteristic p^r. According to [7] every finite chain ring is of the form:

$$R = GR(p^n, r)[X]/(g, p^{n-1}x^t);$$

where $GR(p^n, r)$ is a Galois extension of $\mathbb{F}_{p^n}$ of degree r and $g \in GR(p^n, r)[x]$ is an Eisenstein polynomial of degree e. The five integers (p, n, r, e, t) associated to the finite chain ring R are called the invariant of R.

Finite commutative chain rings can also be constructed from p-adic fields since finite commutative chain rings are the nontrivial quotients of rings of integers of p-adic fields see [4] and [5]. The next proposition summarize the connection between p-adic fields and finite chain rings. The reference [7] contains the general background of finite commutative chain rings.

Proposition .4: [5] Let K be a finite extension of $\mathbb{Q}_p$ such that $[K : \mathbb{Q}_p] = n$ with residue degree r and ramification index e. Let $\mathcal{O}_K$ be the ring of integers of K and π a prime of K then

$$\mathcal{O}_K/\pi^s\mathcal{O}_K \cong GR(p^n, r)[X]/(g, p^{n-1}x^t).$$

A linear code over a finite chain ring R is a submodule of R. Let C be a linear code of length n over R, we assume that n is not divisible by the characteristic of the residue field $R/M = \mathbb{F}_{p^r}$.

Definition .5: (**Generator matrix, type and rank of a linear code** C) [8]

Let C be a code over R. A matrix G is called a generator matrix for C if the rows of G span C and none of them can be written as an $R-$linear combination of other rows of G. We say that G is a generator matrix in standard form if

$$G = \begin{pmatrix} I_{k_0} & A_{0,1} & A_{0,2} & A_{0,3} & \cdots & \cdots & A_{0,s} \\ 0 & \pi I_{K_1} & \pi A_{1,2} & \pi A_{1,3} & \cdots & \cdots & \pi A_{1,s} \\ 0 & 0 & \pi^2 I_{k_2} & \pi^2 A_{2,3} & \cdots & \cdots & \pi^2 A_{2,s} \\ \vdots & \vdots & 0 & \ddots & \ddots & & \vdots \\ \vdots & \vdots & \vdots & \ddots & \ddots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & \cdots & \pi^{s-1} I_{k_{s-1}} & \pi^{s-1} A_{s-1,s} \end{pmatrix} \quad (1)$$

where the columns are grouped into blocks of sizes $k_0, k_1, ..., k_{s-1}, n - \sum_{i=0}^{e-1} k_i$. We say that C is of type $1^{k_0}\pi^k - 1(\pi^2)^{k_2}...(\pi^{s-1})^{k_{e-1}}$. We have the following equality

$$|C| = |M|^{\sum_{i=0}^{s-1}(e-i)k_i}.$$

The rank of C is defined to be

$$k(C) = \Sigma_{i=0}^{s-1} k_i.$$

So the type and the rank are the invariant of C.

A linear code C is said to be free if its rank is equal to the maximum of the ranks of the free submodules of C, then we have that the code C is a free R-submodule which is isomorphic as a module to $R^{k(C)}$, and has a basis of $k(C)$ elements as for codes over finite fields.

The Dual-Code: We attach the standard inner product to the ambient space, i.e., $x \cdot y = \sum x_i y_i$. The dual code $C^\perp$ of C is defined by $C^\perp = \{x \in R^n; x \cdot y = 0 \textit{ for all } y \in C\}$. If $C \subseteq C^\perp$ we say that the code is self-orthogonal, and if $C = C^\perp$ we say that the code is self-dual.

A. Lifted Codes

Let Ω be an algebraic closure of $\mathbb{Q}_p$ and let K be a finite extension of $\mathbb{Q}_p$ of degree n.

We define

$$R_i = \mathcal{O}_K/\pi^i\mathcal{O}_K = \{a_0 + a_1\pi^1 + ... + a_{i-1}\pi^{i-1}\}; a_i \in \mathcal{O}_K.$$

Since every finite chain ring is isomophic to a non-trivial quotients of rings of integers of p-adic fields, then the R_i are finite chain ring, then we have the next lemma

Lemma .1: The ring R_i is a finite chain ring with maximal ideal $\langle\pi\rangle$.

The ring of formel power series in x with coefficient in a finite chain ring R is defined to be the ring of elements with infinite expressions of the following form

$$a(x) = \sum_{i=0}^{\infty} a_i x^i \ ; \ a_i \in R \textit{ for all } i \in \mathbb{N}.$$

We denote it by $R[[x]]$, the addition and multiplication operator are defined as for the ring of polynomials.

We define the ring of power series in π with coefficient in a finite chain ring $R = \mathcal{O}_K/\pi^s\mathcal{O}_K$ as follow

$$R_\infty = \{\sum_{i=0}^{\infty} a_i\pi^i \ ; \ a_i \in \mathcal{O}_K\}$$

In the next theorem we investigate the definition of formel power series and the connection between finite chain rings and nontrivial rings of integers of p-adic fields to give a generalisation of the construction given in [2].

Theorem .2: The ring of formel power series in π with coefficient in a nontrivial quotients of rings of integers of K is the ring of integers of K:

$$R_\infty = \mathcal{O}_K.$$

Proof .1: $R_\infty = \{\sum_{i=0}^{\infty} a_i\pi^i \ ; \ a_i \in \mathcal{O}_K\}$ We have that every element $\alpha \in \mathcal{O}_K$ can be written in a unique way $\alpha = \sum_{j=0}^{\infty} b_j\pi^j \ ; \ b_j \in \mathbb{F}_{p^r}$, then

$$R_\infty = \{\sum_{i=0}^{\infty}(\sum_{j=0}^{\infty} b_j\pi^j)\pi^i\} = \{\sum_{s=0}^{\infty}(\sum_{i+j=s} b_{ij})\pi^s \ ; \ b_{ij} \in \mathbb{F}_{p^r}\}.$$

by letting $a_s = \sum_{i+j=s} b_{ij}$ with $b_{ij} \in \mathbb{F}_{p^r}$ and we have that $\sum_{i+j=s} b_{ij}$ with $b_{ij} \in \mathbb{F}_{p^r}$ is a finite sum then

$$R_\infty = \{\sum_{s}^{\infty} a_s\pi^s \ ; \ a_s \in \mathbb{F}_{p^r}\} = \mathcal{O}_K.$$

Proposition .5: $\mathcal{O}_K$ is a Noetherian ring.

Proof .2: According to [6] we have that the ideals of $\mathcal{O}_K$ form the next sequence:

$$\{0\} \subset \cdots \langle\pi^n\rangle \subset \cdots \subset \langle\pi^2\rangle \subset \langle\pi\rangle \subset \langle\pi^0\rangle = \mathcal{O}_K$$

then R_∞ satisfies the ascending chain condition, i.e; R_∞ is a Noetherian ring.

Proposition .6: $\mathcal{O}_K$ is a Euclidean domain.

Proof .3: To verify the Euclidean property :

If a and $b \neq 0$ are in R_∞, then there exist q and r in R_∞ such that $a = bq + r$ and either $r = 0$ or $f(r) < f(b)$, where f is a function from R_∞ to $\mathbb{Z}^+$. We let $V : R_\infty \to \mathbb{Z}^+$ to be the function defined by $V(0) = 0$ and $V(r) = v(r)$ if $r \neq 0$. If $v(a) \geq v(b)$ then $v(a/b) = v(a)_v(b) \geq 0$ if we we put $q = a/b \in R_\infty$ we can let $r = 0$. Now if $v(a) < v(b)$; then we can let $q = 0$ and $r = a$. So R_∞ is a Euclidean domain. Since any Euclidean domain is also a Dedekind domain, then we deduce the next proposition

Proposition .7: $\mathcal{O}_K$ is a Dedekind domain.

A linear code of length n and rank k over R_∞ is called π-adic $[n, k]$-code.

Lemma .2: [2] Let C be a nonzero linear code over R_∞ of length n, then any generator matrix of C is permutation equivalent to a matrix of the following form:

$$\begin{pmatrix} \pi^{m_0}I_{k_0} & \pi^{m_0}A_{0,1} & \pi^{m_0}A_{0,2} & \pi^{m_0}A_{0,3} & & & \pi^{m_0}A_{0,r} \\ & \pi^{m_1}I_{k_1} & \pi^{m_1}A_{1,2} & \pi^{m_1}A_{1,3} & & & \pi^{m_1}A_{1,r} \\ & & \pi^{m_2}I_{k_2} & \pi^{m_2}A_{2,3} & & & \pi^{m_2}A_{2,r} \\ & & & \ddots & \ddots & & \\ & & & & \ddots & \ddots & \\ & & & & & \pi^{m_{r-1}}I_{k_{r-1}} & \pi^{m_{r-1}}A_{r-1,r} \end{pmatrix} \tag{2}$$

The code C with generator matrix of this form is said to be of type

$$(\pi^{m_0})^{k_0}(\pi^{m_1})^{k_1}\cdots(\pi^{m_{r-1}})^{k_{r-1}},$$

where $k = k_0+k_1+\cdots+k_{r-1}$ is called its rank and $k_r = n-k$.

Definition .6:

A cyclic code of length m over the ring of integers $\mathcal{O}_K$ is a linear code such that if $(c_0, c_1, \cdots, c_{m-1}) \in C$, then $(c_{m-1}, c_0, \cdots, c_{m-2}) \in C$.

The codewords of a cyclic code over $\mathcal{O}_K$ are represented as usual by polynomials, more precisely they are the ideals of the ring $\mathcal{O}_K/\langle X^n - 1\rangle$.

For tow integers $i < j$, we define a map as in [2] as follow:

$$\begin{aligned} &\Psi_i^j : R_j \to R_i \\ &\sum_{l=0}^{j-1} a_l\pi^l \mapsto \sum_{l=0}^{i-1} a_l\pi^l. \end{aligned} \tag{3}$$

If we replace R_j with R_∞ then we denote Ψ_i^∞ by Ψ_i. For two element $a, b \in R_\infty$, we have that

$$\Psi_i(a+b) = \Psi_i(a) + \Psi_i(b), \ \Psi_i(ab) = \Psi_i(a)\Psi_i(b).$$

The two maps Ψ_i and Ψ_i^j can be extended naturally from R_∞^n to R_i^n and R_j^n to R_i^n respectively.

Remark 1: From the above construction given by (3) we get the next series of chain rings as follows:

$$R_\infty \to \cdots \to R_s \cdots \to R_{s-1} \to R_m \to \cdots \to R_1$$

where

- $R_1 = \mathcal{O}_K/\pi\mathcal{O}_K \cong \mathbb{F}_{p^r}$
- $R_m = \mathcal{O}_K/\pi^m\mathcal{O}_K$
- $R_{s-1} = \mathcal{O}_K/\pi^{s-1}\mathcal{O}_K$

- $R_s = \mathcal{O}_K/\pi^s\mathcal{O}_K$
- $R_\infty = \mathcal{O}_K$

for $1 \leq t^{'} \leq t \leq e$ (e is the degree of the Eisenstein polynomial g)

Now we define the lifts of a code over a finite chain ring.

Definition .7: [2] Let i, j be two integers such that $1 \leq i \leq j < \infty$. We say that an $[n, k]$ code C_1 over R_i lifts to an $[n, k]$ code C_2 over R_j, denoted by $C_1 \leq C_2$, if C_2 has a generator matrix G_2 such that $\Psi_i^j(G_2)$ is a generator matrix of C_1. It can be proven that $C_1 = \Psi_i^j(C_2)$. If C is a $[n, k]$ π-adic code, then for any $i < \infty$, we call $\Psi_i(C)$ the projection of C. We denote $\Psi_i(C)$ by C^i.

Lemma .3: Let C be a linear code over R_i and $\tilde{C}$ be the lifted code of C over R_j, where $i < j \leqslant \infty$. Then if C is free over R_i then $\tilde{C}$ is free over R_j.

REFERENCES

[1] Calderbank S. Sloane N. J. A., Modular and p-adic cyclic codes, Designs, codes and cryptography, vol. 6, pp.21-35, 1995.

[2] S. T. Dougherty, H. Liu, and Park Y. H.,Lifted codes over finite chain rings, Mathematical Journal of Okayama University, Vol. 53, pp.39-53, January 2010, .

[3] K. Guenda, T. A. Gulliver, MDS and self-dual codes over rings, Finite Fields and Their Applications, vol. 18, pp. 1061-1075, 2012, .

[4] X. Hou and K. H. Leung, and S. L. Ma, On the groups of units of finite commutative chain rings, Finite Fields and their applications, vol. 9, pp.20-38, 2003.

[5] Hou X. and Keating K., Enumeration of isomorphism classes of extensions of p-adic fields, Journal of Number Theory, vol. 104, pp.14-61, 2004, .

[6] Iwasawa K., Local class field theory, Oxford university press, 1986.

[7] McDonald B.R., Finite Rings with Identity, Marcel Dekker, New York, 1974.

[8] Norton G.H., Sălăgean, On the structure of linear and cyclic codes over finite chain rings, Applicable algebra in ingineering, communication and computing, vol. 10, pp.489-506, 2000.

[9] Serre J.P., Local Fields, Graduate Texts in Mathematics, Springer, 1979.

Three-Weight Minimal Linear Codes and Their Applications

Sihem Mesnager
Department of Mathematics
Universities of Paris VIII and XIII
CNRS, UMR 7539 LAGA
and Telecom ParisTech,
Paris, France
smesnager@univ-paris8.fr

Ahmet Sınak
Department of Mathematics and Computer
Necmettin Erbakan University
LAGA, UMR 7539, CNRS
Universities of Paris VIII and XIII, France.
sinakahmet@gmail.com

Oğuz Yayla
Department of Mathematics
Hacettepe University
Ankara, Turkey
oguz.yayla@hacettepe.edu.tr

***Abstract*—Minimal linear codes have important applications in secret sharing schemes and secure two-party computation. In this paper, we first construct linear codes with three weights from weakly regular plateaued functions based on the second generic construction and determine their weight distributions. We next give punctured version of each constructed codes. We also observe that the constructed codes in this paper are minimal for almost all cases. We finally describe the access structures of the secret sharing schemes based on the dual codes of the constructed minimal codes.**

***Index Terms*—Minimal codes, weakly regular plateaued functions, secret sharing schemes**

I. Introduction

For a prime number p and a positive integer n, the finite field with p^n elements is denoted by $\mathbb{F}_{p^n}$. The finite field $\mathbb{F}_{p^n}$ can be viewed as an n-dimensional vector space over $\mathbb{F}_p$, denoted by $\mathbb{F}_p^n$. A linear code $\mathcal{C}$ of length n and dimension k over $\mathbb{F}_p$ is a k-dimensional linear subspace of $\mathbb{F}_p^n$. An element of $\mathcal{C}$ is said to be a *codeword*. The Hamming weight of a vector $\mathbf{a}=(a_0,\ldots,a_{n-1})\in\mathbb{F}_p^n$, denoted by $wt(\mathbf{a})$, is the size of its support defined as $\mathrm{supp}(\mathbf{a})=\{0\le i\le n-1 : a_i\neq 0\}$. The minimum Hamming distance of $\mathcal{C}$ is the minimum Hamming weight of its nonzero codewords. A linear code $\mathcal{C}$ of length n and dimension k over $\mathbb{F}_p$ with minimum Hamming distance d is denoted by $[n,k,d]_p$. Let A_w denote the number of codewords with Hamming weight w in $\mathcal{C}$ of length n. Then, $(1,A_1,\ldots,A_n)$ is the *weight distribution* of $\mathcal{C}$ and the polynomial $1+A_1y+\cdots+A_ny^n$ is called the *weight enumerator* of $\mathcal{C}$. The code $\mathcal{C}$ is called a *t-weight code* if the number of nonzero A_w in the weight distribution is t. We say that a codeword $\mathbf{a}$ of $\mathcal{C}$ covers another codeword $\mathbf{b}$ of $\mathcal{C}$ if $\mathrm{supp}(\mathbf{a})$ contains $\mathrm{supp}(\mathbf{b})$. A nonzero codeword $\mathbf{a}$ of $\mathcal{C}$ is said to be *minimal* if $\mathbf{a}$ covers only the codeword $j\mathbf{a}$ for every $j\in\mathbb{F}_p$, but no other nonzero codewords of $\mathcal{C}$. A linear code $\mathcal{C}$ is said to be *minimal* if every nonzero codeword of $\mathcal{C}$ is minimal.

Herein after, we fix the following notations unless otherwise stated. For any set E, $\#E$ denotes the cardinality of E and $E^\star=E\backslash\{0\}$. SQ and NSQ denote respectively the set of all squares and non-squares in $\mathbb{F}_p^\star$. We denote by η_0 the quadratic character of $\mathbb{F}_p^\star$, and $p^*=\eta_0(-1)p$. The trace of $\alpha\in\mathbb{F}_{p^n}$ over $\mathbb{F}_p$ is defined as $\mathrm{Tr}^n(\alpha)=\alpha+\alpha^p+\alpha^{p^2}+\cdots+\alpha^{p^{n-1}}$. Given a function $f:\mathbb{F}_{p^n}\longrightarrow\mathbb{F}_p$, the Walsh transform of f is defined by:

$$\widehat{\chi_f}(\omega)=\sum_{x\in\mathbb{F}_{p^n}}\xi_p^{f(x)-\mathrm{Tr}^n(\omega x)},$$

where $\xi_p=e^{2\pi i/p}$ is a complex primitive p-th root of unity. The notion of plateaued functions was first introduced in characteristic 2 by Zheng and Zhang (1999) [17]. In characteristic p, a function f is said to be p-ary s-plateaued if $|\widehat{\chi_f}(\beta)|^2\in\{0,p^{n+s}\}$ for every $\beta\in\mathbb{F}_{p^n}$, where s is an integer with $0\le s\le n$. An s-plateaued f is said to be *weakly regular* if there exists a complex number u having unit magnitude such that $\widehat{\chi_f}(\beta)\in\{0,up^{\frac{n+s}{2}}\xi_p^{g(\beta)}\}$ for all $\beta\in\mathbb{F}_{p^n}$, where g is a p-ary function over $\mathbb{F}_{p^n}$ with $g(\beta)=0$ for all $\beta\in\mathbb{F}_{p^n}\setminus\mathrm{Supp}(\widehat{\chi_f})$; otherwise, f is said to be *non-weakly regular* [9]. In particular, weakly regular plateaued f is said to be *regular* if $u=1$. A function f is said to be *balanced* over $\mathbb{F}_p$ if f takes every value of $\mathbb{F}_p$ the same number of p^{n-1} times, in other words, $\widehat{\chi_f}(0)=0$; otherwise, f is called *unbalanced*. It is worth noting that plateaued (but not bent) functions may be balanced or unbalanced. The Walsh support of plateaued f is defined by $\mathrm{Supp}(\widehat{\chi_f})=\{\beta\in\mathbb{F}_{p^n}:|\widehat{\chi_f}(\beta)|^2=p^{n+s}\}$ and $\#\mathrm{Supp}(\widehat{\chi_f})=p^{n-s}$.

Lemma 1. *Let $f:\mathbb{F}_{p^n}\to\mathbb{F}_p$ be an s-plateaued function. Then for $\beta\in\mathbb{F}_{p^n}$, $|\widehat{\chi_f}(\beta)|^2$ takes p^{n-s} times the value p^{n+s} and p^n-p^{n-s} times the value 0.*

Lemma 2. *[9] Let $f:\mathbb{F}_{p^n}\to\mathbb{F}_p$ be a weakly regular s-plateaued function. For all $\beta\in\mathrm{Supp}(\widehat{\chi_f})$, we have $\widehat{\chi_f}(\beta)=\epsilon\sqrt{p^*}^{n+s}\xi_p^{g(\beta)}$, where $\epsilon=\pm1$ is the sign of $\widehat{\chi_f}$ and g is a p-ary function over $\mathrm{Supp}(\widehat{\chi_f})$.*

Lemma 3. *[10] Let f be a weakly regular s-plateaued function with $\widehat{\chi_f}(\beta)=\epsilon\sqrt{p^*}^{n+s}\xi_p^{g(\beta)}$ for every $\beta\in\mathrm{Supp}(\widehat{\chi_f})$. For $j\in\mathbb{F}_p$, define $\mathcal{N}_g(j)=\#\{\beta\in\mathrm{Supp}(\widehat{\chi_f}):g(\beta)=j\}$. Then, if $n-s$ is even,*

$$\mathcal{N}_g(j)=\begin{cases}p^{n-s-1}+\epsilon\eta_0^{n+1}(-1)(p-1)\sqrt{p^*}^{n-s-2}, & \text{if } j=0,\\ p^{n-s-1}-\epsilon\eta_0^{n+1}(-1)\sqrt{p^*}^{n-s-2}, & \text{if } j\in\mathbb{F}_p^\star,\end{cases}$$

if $n-s$ is odd,

$$\mathcal{N}_g(j)=\begin{cases} p^{n-s-1}, & \text{if } j=0,\\ p^{n-s-1}+\epsilon\eta_0^n(-1)\sqrt{p^*}^{n-s-1}, & \text{if } j\in SQ,\\ p^{n-s-1}-\epsilon\eta_0^n(-1)\sqrt{p^*}^{n-s-1}, & \text{if } j\in NSQ.\end{cases}$$

II. Linear codes from weakly regular plateaued functions

In this section, we partially generalize the construction method of binary linear codes from Boolean functions proposed by C. Ding [4], [5] to weakly regular plateaued functions in characteristic p, based on the second generic construction. Let f be a p-ary function from $\mathbb{F}_{p^n}$ to $\mathbb{F}_p$. The *support* of f is defined to be a set

$$D_f=\{x\in\mathbb{F}_{p^n}: f(x)\neq 0\}\subseteq\mathbb{F}_{p^n}. \tag{1}$$

Assume $n_f=\#D_f$ and $D_f=\{d_1,d_2,\ldots,d_{n_f}\}$. The second generic construction of linear codes from functions is obtained from D_f and a linear code involving D_f is defined by

$$\mathcal{C}_{D_f}=\{c_\beta=(\mathrm{Tr}^n(\beta d_1),\ldots,\mathrm{Tr}^n(\beta d_{n_f})):\beta\in\mathbb{F}_{p^n}\}. \tag{2}$$

A. Linear codes from weakly regular plateaued unbalanced functions

In this subsection, to construct p-ary linear codes, we make use of weakly regular plateaued unbalanced functions in characteristic p.

We first recall from [10] that *WRP* denotes the set of weakly regular p-ary plateaued unbalanced functions $f:\mathbb{F}_{p^n}\to\mathbb{F}_p$ satisfying the following two homogeneous conditions: $f(0)=0$ and there exists a positive integer t with $\gcd(t-1,p-1)=1$ such that $f(ax)=a^tf(x)$ for any $a\in\mathbb{F}_p^\star$ and $x\in\mathbb{F}_{p^n}$.

The following lemma can be obviously derived from [10, Lemma 11].

Lemma 4. *Let $f:\mathbb{F}_{p^n}\to\mathbb{F}_p$ be an unbalanced function with $\widehat{\chi_f}(0)=\epsilon\sqrt{p^*}^{n+s}$, where $\epsilon=\pm1$. Then,*

$$n_f=\begin{cases}(p-1)(p^{n-1}-\epsilon\eta_0(-1)\sqrt{p^*}^{n+s-2}), & \text{if } n+s \text{ is even,}\\ (p-1)p^{n-1}, & \text{if } n+s \text{ is odd.}\end{cases}$$

The following lemma follows directly from [10, Lemma 15].

Lemma 5. *Let $f\in$ WRP and define $\mathcal{N}_{f,\beta}=\#\{x\in\mathbb{F}_{p^n}: f(x)\neq 0$ and $\mathrm{Tr}^n(\beta x)=0\}$ for $\beta\in\mathbb{F}_{p^n}^\star$. Then for every $\beta\in\mathbb{F}_{p^n}^\star\setminus\mathrm{Supp}(\widehat{\chi_f})$, we have*

$$\mathcal{N}_{f,\beta}=\begin{cases}(p-1)\left(p^{n-2}-\epsilon\sqrt{p^*}^{n+s-4}\right), & \text{if } n+s \text{ is even,}\\ (p-1)p^{n-2}, & \text{if } n+s \text{ is odd,}\end{cases}$$

and for every $\beta\in\mathrm{Supp}(\widehat{\chi_f})$, if $n+s$ is even, then

$$\mathcal{N}_{f,\beta}=\begin{cases}(p-1)\left(p^{n-2}-\epsilon\eta_0(-1)\sqrt{p^*}^{n+s-2}\right), & \text{if } g(\beta)=0,\\ (p-1)p^{n-2}, & \text{if } g(\beta)\neq 0,\end{cases}$$

if $n+s$ is odd, then

$$\mathcal{N}_{f,\beta}=\begin{cases}(p-1)p^{n-2}, & \text{if } g(\beta)=0,\\ (p-1)\left(p^{n-2}-\epsilon\sqrt{p^*}^{n+s-3}\right), & \text{if } g(\beta)\in SQ,\\ (p-1)\left(p^{n-2}+\epsilon\sqrt{p^*}^{n+s-3}\right), & \text{if } g(\beta)\in NSQ.\end{cases}$$

We derive from Lemma 5 the Hamming weights of the codewords of $\mathcal{C}_{D_f}$ and determine its weight distribution by Lemmas 1 and 3.

Theorem 1. *Let $n+s$ be even and $f\in$ WRP. Then $\mathcal{C}_{D_f}$ is the three-weight linear code with parameters $[(p-1)(p^{n-1}-\epsilon\eta_0(-1)\sqrt{p^*}^{n+s-2}),n]$. The Hamming weights of the codewords and the weight distribution of $\mathcal{C}_{D_f}$ are as in Table I, where $\epsilon=\pm1$ is the sign of $\widehat{\chi_f}$.*

Notice that Theorem 1 is a partial extension of [5, Corollaries 3 and 5] to weakly regular plateaued functions in characteristic p.

Theorem 2. *Let $n+s$ be odd and $f\in$ WRP. Then, $\mathcal{C}_{D_f}$ is the three-weight linear code with parameters $[(p-1)p^{n-1},n]$. The Hamming weights of the codewords and the weight distribution of $\mathcal{C}_{D_f}$ are as in Table II.*

Proof. From the definition of $\mathcal{C}_{D_f}$, we have $n_f=(p-1)p^{n-1}$ by Lemma 4 and $wt(c_\beta)=n_f-\mathcal{N}_{f,\beta}$ for every $\beta\in\mathbb{F}_{p^n}^\star$ by Lemma 5. Hence for every $\beta\in\mathbb{F}_{p^n}^\star\setminus\mathrm{Supp}(\widehat{\chi_f})$, $wt(c_\beta)=(p-1)^2p^{n-2}$, and the number of such codewords c_β is p^n-p^{n-s} by Lemma 1. For every $\beta\in\mathrm{Supp}(\widehat{\chi_f})$, we get

$$wt(c_\beta)=\begin{cases}(p-1)^2p^{n-2}, & \text{if } g(\beta)=0,\\ (p-1)^2p^{n-2}+\epsilon(p-1)\sqrt{p^*}^{n+s-3}, & \text{if } g(\beta)\in SQ,\\ (p-1)^2p^{n-2}-\epsilon(p-1)\sqrt{p^*}^{n+s-3}, & \text{if } g(\beta)\in NSQ,\end{cases}$$

and the number of such codewords c_β follows from Lemma 3. □

B. Linear codes from weakly regular plateaued balanced functions

In this subsection, we make use of weakly regular plateaued balanced functions to obtain further p-ary linear codes.

We denoted in [15] by *WRPB* the set of weakly regular p-ary plateaued balanced functions $f:\mathbb{F}_{p^n}\to\mathbb{F}_p$ satisfying the following two homogeneous conditions: $f(0)=0$ and there exists a positive even integer t with $\gcd(t-1,p-1)=1$ such that $f(ax)=a^tf(x)$ for any $a\in\mathbb{F}_p^\star$ and $x\in\mathbb{F}_{p^n}$.

Remark 1. If $f:\mathbb{F}_{p^n}\to\mathbb{F}_p$ is a balanced function, then $n_f=(p-1)p^{n-1}$.

The following lemma follows directly from [15, Lemma 7].

Lemma 6. *Let $f\in$ WRPB and define $\mathcal{N}_{f,\beta}=\#\{x\in\mathbb{F}_{p^n}: f(x)\neq 0$ and $\mathrm{Tr}^n(\beta x)=0\}$ for $\beta\in\mathbb{F}_{p^n}^\star$. Then for every $\beta\in\mathbb{F}_{p^n}^\star\setminus\mathrm{Supp}(\widehat{\chi_f})$, we have $\mathcal{N}_{f,\beta}=(p-1)p^{n-2}$ and for every $\beta\in\mathrm{Supp}(\widehat{\chi_f})$, if $n+s$ is even, then*

$$\mathcal{N}_{f,\beta}=\begin{cases}(p-1)(p^{n-2}-\epsilon(p-1)\sqrt{p^*}^{n+s-4}), & \text{if } g(\beta)=0,\\ (p-1)(p^{n-2}+\epsilon\sqrt{p^*}^{n+s-4}), & \text{if } g(\beta)\neq 0,\end{cases}$$

if $n+s$ is odd, then

$$\mathcal{N}_{f,\beta}=\begin{cases}(p-1)p^{n-2}, & \text{if } g(\beta)=0,\\ (p-1)(p^{n-2}-\epsilon\sqrt{p^*}^{n+s-3}), & \text{if } g(\beta)\in SQ,\\ (p-1)(p^{n-2}+\epsilon\sqrt{p^*}^{n+s-3}), & \text{if } g(\beta)\in NSQ.\end{cases}$$

We derive from Lemma 6 the Hamming weights of the codewords of $\mathcal{C}_{D_f}$ and determine its weight distribution by Lemmas 1 and 3.

Table I
THE WEIGHT DISTRIBUTION OF $\mathcal{C}_{D_f}$ WHEN $n+s$ IS EVEN

Hamming weight w	Multiplicity A_w
0	1
$(p-1)^2\left(p^{n-2}-\epsilon\sqrt{p^*}^{n+s-4}\right)$	p^n-p^{n-s}
$(p-1)^2p^{n-2}$	$p^{n-s-1}+\epsilon\eta_0^{n+1}(-1)(p-1)\sqrt{p^*}^{n-s-2}-1$
$(p-1)((p-1)p^{n-2}-\epsilon\eta_0(-1)\sqrt{p^*}^{n+s-2})$	$(p-1)\left(p^{n-s-1}-\epsilon\eta_0^{n+1}(-1)\sqrt{p^*}^{n-s-2}\right)$

Table II
THE WEIGHT DISTRIBUTION OF $\mathcal{C}_{D_f}$ WHEN $n+s$ IS ODD

Hamming weight w	Multiplicity A_w
0	1
$(p-1)^2p^{n-2}$	$p^n+p^{n-s-1}-p^{n-s}-1$
$(p-1)((p-1)p^{n-2}+\epsilon\sqrt{p^*}^{n+s-3})$	$\frac{p-1}{2}\left(p^{n-s-1}+\epsilon\eta_0^n(-1)\sqrt{p^*}^{n-s-1}\right)$
$(p-1)((p-1)p^{n-2}-\epsilon\sqrt{p^*}^{n+s-3})$	$\frac{p-1}{2}\left(p^{n-s-1}-\epsilon\eta_0^n(-1)\sqrt{p^*}^{n-s-1}\right)$

Theorem 3. *Let $n+s$ be even and $f \in$ WRPB. Then $\mathcal{C}_{D_f}$ is the three-weight linear code with parameters $[(p-1)p^{n-1}, n]$. The Hamming weights of the codewords and the weight distribution of $\mathcal{C}_{D_f}$ are as in Table III.*

Proof. From the definition of $\mathcal{C}_{D_f}$, its length is $n_f = (p-1)p^{n-1}$ by Remark 1 and for every $\beta \in \mathbb{F}_{p^n}^\star$, the Hamming weight of its codeword $\mathbf{c}_\beta$ is

$$wt(c_\beta) = n_f - \mathcal{N}_{f,\beta},$$

where $\mathcal{N}_{f,\beta}$ is given by Lemma 6. For every $\beta \in \mathbb{F}_{p^n}^\star \setminus \mathrm{Supp}(\widehat{\chi_f})$, $wt(c_\beta) = (p-1)^2p^{n-2}$ and the number of such codewords c_β is $p^n - p^{n-s} - 1$ by Lemma 1. For every $\beta \in \mathrm{Supp}(\widehat{\chi_f})$, we obtain

$$wt(c_\beta) = \begin{cases} (p-1)^2(p^{n-2}+\epsilon\sqrt{p^*}^{n+s-4}), & \text{if } g(\beta)=0, \\ (p-1)((p-1)p^{n-2}-\epsilon\sqrt{p^*}^{n+s-4}), & \text{if } g(\beta)\neq 0, \end{cases}$$

and the number of such codewords c_β follows from Lemma 3. □

Notice that Theorem 3 is a partial extension of [5, Corollary 5] to weakly regular plateaued functions in characteristic p.

Remark 2. In the case of $n+s$ is odd, then $\mathcal{C}_{D_f}$ has the same parameters and weight distribution of the linear code $\mathcal{C}_{D_f}$ of Theorem 2.

C. The punctured versions of the constructed codes

In this subsection, we deal with the punctured versions of the constructed codes above.

The code $\mathcal{C}_{D_f}$ defined by (2) can be punctured into a shorter one whose weight distribution is derived from that of $\mathcal{C}_{D_f}$ since the Hamming weights of all nonzero codewords of $\mathcal{C}_{D_f}$ have a common divisor $p-1$. Let $f \in WRP$ or $WRPB$. For any $x \in \mathbb{F}_{p^n}$, $f(x) = 0$ if and only if $f(ax) = 0$, for every $a \in \mathbb{F}_p^\star$. Then one can choose a subset $\bar{D}_f$ of the defining set D_f defined by (1) such that $\bigcup_{a\in\mathbb{F}_p^\star} a\bar{D}_f$ is a partition of D_f, namely,

$$D_f = \mathbb{F}_p^\star \bar{D}_f = \{a\bar{d} : a \in \mathbb{F}_p^\star \text{ and } \bar{d} \in \bar{D}_f\}, \tag{3}$$

where for each pair of distinct elements $\bar{d}_1, \bar{d}_2 \in \bar{D}_f$ we have $\frac{\bar{d}_1}{\bar{d}_2} \notin \mathbb{F}_p^\star$. This implies that the linear code $\mathcal{C}_{D_f}$ can be punctured into a shorter linear code $\mathcal{C}_{\bar{D}_f}$, which is defined as in (2) for the defining set $\bar{D}_f$. Hence, the following linear codes in Corollaries 1, 2 and 3 are directly obtained from the constructed ones in Theorems 1, 2 and 3, respectively.

Corollary 1. *The punctured version $\mathcal{C}_{\bar{D}_f}$ of the code $\mathcal{C}_{D_f}$ of Theorem 1 is the three-weight linear code with parameters $\left[p^{n-1}-\epsilon\eta_0(-1)\sqrt{p^*}^{n+s-2}, n\right]_p$ whose weight distribution is listed in Table IV.*

Corollary 2. *The punctured version $\mathcal{C}_{\bar{D}_f}$ of the code $\mathcal{C}_{D_f}$ of Theorem 2 is the three-weight linear code with parameters $\left[p^{n-1}, n\right]_p$ whose weight distribution is listed in Table V.*

Corollary 3. *The punctured version $\mathcal{C}_{\bar{D}_f}$ of the code $\mathcal{C}_{D_f}$ of Theorem 3 is the three-weight linear code with parameters $\left[p^{n-1}, n\right]_p$ whose weight distribution is listed in Table VI.*

III. SECRET SHARING SCHEMES FROM THE CONSTRUCTED LINEAR CODES

In this section, we first show that the constructed codes in this paper are minimal and next describe the access structures of the secret sharing schemes based on their dual codes.

A. The minimality of the constructed linear codes

With the help of Lemma 7, we can easily observe that all nonzero codewords of the constructed codes are minimal, which completes the proofs of the following corollaries.

Lemma 7. *(Ashikhmin-Barg) [1] All nonzero codewords of a linear code $\mathcal{C}$ over $\mathbb{F}_p$ are minimal if*

$$\frac{p-1}{p} < \frac{w_{\min}}{w_{\max}},$$

Table III
THE WEIGHT DISTRIBUTION OF $\mathcal{C}_{D_f}$ WHEN $n+s$ IS EVEN

Hamming weight w	Multiplicity A_w
0	1
$(p-1)^2p^{n-2}$	$p^n-p^{n-s}-1$
$(p-1)^2(p^{n-2}+\epsilon\sqrt{p^*}^{n+s-4})$	$p^{n-s-1}+\epsilon\eta_0^{n+1}(-1)(p-1)\sqrt{p^*}^{n-s-2}$
$(p-1)((p-1)p^{n-2}-\epsilon\sqrt{p^*}^{n+s-4})$	$(p-1)\left(p^{n-s-1}-\epsilon\eta_0^{n+1}(-1)\sqrt{p^*}^{n-s-2}\right)$

Table IV
THE WEIGHT DISTRIBUTION OF $\mathcal{C}_{\bar{D}_f}$ WHEN $n+s$ IS EVEN

Hamming weight w	Multiplicity A_w
0	1
$(p-1)\left(p^{n-2}-\epsilon\sqrt{p^*}^{n+s-4}\right)$	p^n-p^{n-s}
$(p-1)p^{n-2}$	$p^{n-s-1}+\epsilon\eta_0^{n+1}(-1)(p-1)\sqrt{p^*}^{n-s-2}-1$
$(p-1)p^{n-2}-\epsilon\eta_0(-1)\sqrt{p^*}^{n+s-2}$	$(p-1)\left(p^{n-s-1}-\epsilon\eta_0^{n+1}(-1)\sqrt{p^*}^{n-s-2}\right)$

Table V
THE WEIGHT DISTRIBUTION OF $\mathcal{C}_{\bar{D}_f}$ WHEN $n+s$ IS ODD

Hamming weight w	Multiplicity A_w
0	1
$(p-1)p^{n-2}$	$p^n+p^{n-s-1}-p^{n-s}-1$
$(p-1)p^{n-2}+\epsilon\sqrt{p^*}^{n+s-3}$	$\frac{p-1}{2}\left(p^{n-s-1}+\epsilon\eta_0^n(-1)\sqrt{p^*}^{n-s-1}\right)$
$(p-1)p^{n-2}-\epsilon\sqrt{p^*}^{n+s-3}$	$\frac{p-1}{2}\left(p^{n-s-1}-\epsilon\eta_0^n(-1)\sqrt{p^*}^{n-s-1}\right)$

Table VI
THE WEIGHT DISTRIBUTION OF $\mathcal{C}_{\bar{D}_f}$ WHEN $n+s$ IS EVEN

Hamming weight w	Multiplicity A_w
0	1
$(p-1)p^{n-2}$	$p^n-p^{n-s}-1$
$(p-1)(p^{n-2}+\epsilon\sqrt{p^*}^{n+s-4})$	$p^{n-s-1}+\epsilon\eta_0^{n+1}(-1)(p-1)\sqrt{p^*}^{n-s-2}$
$(p-1)p^{n-2}-\epsilon\sqrt{p^*}^{n+s-4}$	$(p-1)\left(p^{n-s-1}-\epsilon\eta_0^{n+1}(-1)\sqrt{p^*}^{n-s-2}\right)$

where $w_{\min}$ and $w_{\max}$ denote the minimum and maximum weights of nonzero codewords in $\mathcal{C}$, respectively.

Corollary 4. *Let $n+s$ be even and $f \in$ WRP. If $\epsilon\eta_0^{(n+s)/2}(-1)=1$, then the linear code $\mathcal{C}_{D_f}$ of Theorem 1 is minimal with parameters $[(p-1)(p^{n-1}-p^{(n+s-2)/2}), n, (p-1)((p-1)p^{n-2}-p^{(n+s-2)/2})]_p$ when $0 \le s \le n-4$, and $\left[(p-1)(p^{n-1}+p^{(n+s-2)/2}), n, (p-1)^2p^{n-2})\right]_p$, otherwise.*

Corollary 5. *Let $n+s$ be odd with $0 \le s \le n-5$ and $f \in$ WRP. Then the code $\mathcal{C}_{D_f}$ of Theorem 2 is minimal with parameters $\left[(p-1)p^{n-1}, n, (p-1)\left((p-1)p^{n-2}-p^{(n+s-3)/2}\right)\right]_p$.*

Corollary 6. *Let $n+s$ be even with $0 \le s \le n-4$ and $f \in$ WRPB. If $\epsilon\eta_0^{(n+s)/2}(-1)=1$, then the linear code $\mathcal{C}_{D_f}$ of Theorem 3 is minimal with parameters $\left[(p-1)p^{n-1}, n, (p-1)((p-1)p^{n-2}-p^{(n+s-4)/2})\right]_p$ and $\left[(p-1)p^{n-1}, n, (p-1)^2(p^{n-2}-p^{(n+s-4)/2})\right]_p$, otherwise.*

B. Secret sharing schemes from the constructed minimal linear codes

Secret sharing is practically used in many areas. First of all, it can be used in cryptography for secretly sharing an encryption key [2], [14]. Secondly, it is used in cloud computing environment where the encryption key is secretly shared among servers [16]. Third one is in secure multiparty computation (MPC) where computation is based on the secret sharing of all the inputs of the corresponding parties [6]. Another application are of secret sharing schemes is decentralized electronic voting, where the vote of each party is split into different vote-counters, i.e. sharing secret among vote-counters [13]. One of the very recent application of secret sharing scheme is in blockchain technology, where data in blockchain is altered by a group having enough number of secret shares [18].

We now study one of methods of construction secret schemes, in fact we will consider secret schemes from linear

codes. There are a lot of ways to construct sharing schemes from minimal linear codes [7], [8], [11], [12]. We here study the one described in [7].

Let C be a linear code $[n, k, d[_q$ with a generator matrix G having first row g_0. A secret $s \in \mathbb{F}_q$ is shared among n group members as follows. A dealer, one of the group members, chooses a random $u \in \mathbb{F}_{q^k}$ such that $s = ug_0$, and obtains the shares $t = (t_0, \ldots, t_{n-1})$ by obtaining the codeword corresponding to u as $t = uG$. Each components of t are distributed to group members, and t_i is called the secret shares. The secret can be only recovered by a set of secret shares $(t_{i_1}, \ldots, t_{i_m})$ where g_0 is a linear combination of rows $(g_{i_1}, \ldots, g_{i_m})$ of G. In other words, if there is a codeword in the dual of C, denoted by $C^\perp$, starting by 1 and non zero at $(i_1, \ldots, i_m)$ then one can recover s easily. In deed, if one can find the vector $(x_1, \ldots, x_m)$ by solving $\sum_{j=1}^{m} x_j g_{i_j} = g_0$, then $s = \sum_{j=1}^{m} x_j t_{i_j}$.

A set of group members is called the minimal access set if they can recover the secret but any of its proper subsets can not. From the discussion above we say that minimal codewords of $C^\perp$ starting with 1 gives the minimal access sets. And so, minimum distance d of C gives a lower bound on the cardinality of a minimal access set. On the other hand, $d^\perp$ defines the number of minimal access sets for which an arbitrary group involved in. It is well known for linear codes that $d + d^\perp \leq n + 2$. Hence there is a trade of between cardinality of a minimal access set and the number of minimal access sets. Furthermore, it is known that $d + d^\perp = n + 2$ for maximum separable codes (MDS). Hence secret sharing schemes from MDS codes are interesting [11].

The secret sharing schemes based on the dual codes of the constructed minimal codes in this paper have the nice access structures described in [3, Theorem 17], which describes the access structure of a secret sharing scheme based on a dual code of a minimal linear code. As an example, we present the parameters of our scheme for Corollary 4 in the following. One can similarly obtain the access structure parameters for Corollaries 5 and 6.

Proposition 1. *Let $\mathcal{C}_{D_f}$ be the $[(p-1)(p^{n-1} - p^{(n+s-2)/2}), n, (p-1)((p-1)p^{n-2} - p^{(n+s-2)/2})]_p$ code in Corollary 4 with a generator matrix $G = [g_0, g_1, \ldots, g_{m-1}]$. Then in the secret sharing scheme based on $\mathcal{C}_{D_f}^\perp$, the total number of participants is $(p-1)(p^{n-1} - p^{(n+s-2)/2}) - 1$ and there are p^{m-1} minimal-access sets.*

i. *$d^\perp = 2$: If g_i is a multiple of g_0, for some i, then participant P_i must be in every minimal access set; else P_i must be in $(p-1)p^{n-2}$ out of p^{n-1} minimal-access sets.*

ii. *$d^\perp > 2$: For any fixed $t \leq min(n-1, d^\perp - 2)$ every group of t participants is involved in $(p-1)^t p^{n-t-1}$ out of p^{n-1} minimal-access sets.*

IV. Conclusion

In this paper, we obtained several classes of three-weight minimal linear codes from weakly regular plateaued functions with some homogeneous conditions based on the second generic construction. We also determined the weight distributions of the constructed codes. These minimal codes can be directly employed to construct secret sharing schemes with the nice access structures.

References

[1] A. Ashikhmin and A. Barg. Minimal vectors in linear codes. *IEEE Transactions on Information Theory*, 44(5):2010–2017, (1998).

[2] G. R. Blakley et al. Safeguarding cryptographic keys. In *Proceedings of the national computer conference*, volume 48, pages 313–317, 1979.

[3] C. Carlet, C. Ding, and J. Yuan. Linear codes from perfect nonlinear mappings and their secret sharing schemes. *IEEE Transactions on Information Theory*, 51(6):2089–2102, 2005.

[4] C. Ding. Linear codes from some 2-designs. *IEEE Transactions on information theory*, 61(6):3265–3275, 2015.

[5] C. Ding. A construction of binary linear codes from boolean functions. *Discrete mathematics*, 339(9):2288–2303, 2016.

[6] O. Goldreich, S. Micali, and A. Wigderson. How to play any mental game. In *Proceedings of the nineteenth annual ACM symposium on Theory of computing*, pages 218–229. ACM, 1987.

[7] J. L. Massey. Minimal codewords and secret sharing. In *Proceedings of the 6th joint Swedish-Russian international workshop on information theory*, pages 276–279, 1993.

[8] R. J. McEliece and D. V. Sarwate. On sharing secrets and reed-solomon codes. *Communications of the ACM*, 24(9):583–584, 1981.

[9] S. Mesnager, F. Özbudak, and A. Sınak. Linear codes from weakly regular plateaued functions and their secret sharing schemes. *Designs, Codes and Cryptography*, 2018.

[10] S. Mesnager and A. Sınak. Several classes of minimal linear codes with few weights from weakly regular plateaued functions. *arxiv https://arxiv.org/abs/1808.03877v1*, 2018.

[11] J. Pieprzyk and X. Zhang. Ideal secret sharing schemes from mds codes. In *Proc. 5th Int. Conf. Information Security and Cryptology (ICISC 2002)*, pages 269–279, 2002.

[12] A. Renvall and C. Ding. The access structure of some secret-sharing schemes. In *Information Security and Privacy*, pages 67–78. Springer, 1996.

[13] B. Schoenmakers. A simple publicly verifiable secret sharing scheme and its application to electronic voting. In *Annual International Cryptology Conference*, pages 148–164. Springer, 1999.

[14] A. Shamir. How to share a secret. *Communications of the ACM*, 22(11):612–613, 1979.

[15] A. Sınak. Minimal linear codes with few weights and their secret sharing schemes. *Pre-print*, 2019.

[16] C.-N. Yang and J.-B. Lai. Protecting data privacy and security for cloud computing based on secret sharing. In *2013 International Symposium on Biometrics and Security Technologies*, pages 259–266. IEEE, 2013.

[17] Y. Zheng and X.-M. Zhang. Plateaued functions. In *ICICS*, volume 99, pages 284–300. Springer, 1999.

[18] G. Zyskind, O. Nathan, et al. Decentralizing privacy: Using blockchain to protect personal data. In *2015 IEEE Security and Privacy Workshops*, pages 180–184. IEEE, 2015.

New Signature Algorithm Based on Concatenated Rank Codes

Roumaissa Mahdjoubi*, Sedat Akleylek†, Guenda Kenza‡
*Faculty of Mathematics
Univesity of Science and Technology Houari Boumedien
Algiers, Algeria
mahdjoubi.roumaissa@gmail.com
† Ondokuz Mayis University
Samsun, Turkey
sedat.akleylek@bil.omu.edu.tr
‡Faculty of Mathematics
Univesity of Science and Technology Houari Boumedien
Algiers, Algeria
ken.guenda@gmail.com

***Abstract*—In this paper we propose a new rank code based signature scheme that used a concatenation of the LRPC and the λ-Gabidulin codes. Our construction benefits from the decoding algorithm of both of codes a considerable security levels with a moderate public key size.**

***Index Terms*—Rank metric, Signature algorithm, λ-Ganidulin code, LRPC codes.**

I. Introduction

In 1978 McEliece introduced the code based cryptography and opened the problem of finding an efficient signature scheme to solve. Until now, there is no efficient algorithm known due to the large public key of CFS scheme [3] and the large signature size of Fiat-Shamir heuristic [11] and a slow signing algorithm of them. In [12] there was proposed an algorithm which provided a reduced key size from the structure of the codes used but it had a large signature size. Those schemes are not practical since they have to repeat the protocol many times in order to guarantee the correctness and security of the message, and they are vulnerable to attacks such as key recovery and reaction attacks.

In 1991, Gabidulin introduced an analogue to the code based cryptography called rank based cryptography. The main advantage is the reduction of key size of the public key but these codes are very structured. Recently Gaborit et al. [6] proposed a new rank signature algorithm based on LRPC codes similar to NTRU in Hamming metric. It was submitted to the NIST call but it has been withdrawn due to an attack which recover its drawback; the very low weight of the public code's codewords [18]. The main problem that the signatures scheme are based is the Syndrome Decoding problem (SD) which is NP-complete in Hamming metric, while in the rank metric, this problem is proved to be hard in [7]. Many attacks were developed to solve this problem and classified into combinatorial and algebraic attack which are both feasible for specific parameters.

Many Attacks on the signatures schemes were developed such as the information leakage attack and the forgery information attack. They are efficient since they can recover the hidden structure of the public key by the information leaking from real signatures, and the reaction attack that recover the reaction of Bob to recover the structure of the code.

Most efforts in the rank-based cryptography were based on constructing new public key cryptosystems (PKCs) to countering attacks. Recently, Kim et al [13] proposed McNie as a new PKC that submitted to the NIST call [1] and consisted in combining the McElice and the Niederreiter cryptosystems, using parity check matrix of an $[n, k]$ codes in the private key and the generator matrix of an $[n, l]$ linear code in the public key. It benefited from the construction of 3-QC-LRPC and 4-QC-LRPC a major reduction of the key with high security level. Another proposition on a new signature and identification scheme was given by Bellini et al [14], it consisted of two signatures which reduce the public and private keys. But it has a large signature size. In addition with a new Identification scheme that resisted to an attack that was proposed also by the authors which made the Stern and Veron Identification scheme broken. Beside to this, the rank metric code has been enriched with the new construction code named λ-Gabidulin codes proposed by Terry et al. [2], they used such a code in the McEliece-like cryptosystem such that the generator matrix of the public code is multiplied with a scrambler matrix associated to $\lambda \in \mathbb{F}_{q^m}^n$. It is proved to be secure against attacks Overbeck's, anulator polynomial and Frobenious weak attacks [15], [16] and [17].

Our contribution is to provide a new rank signature in code-based cryptography for the λ-Gabidulin code and the LRPC codes by their concatenation. The robustness becomes from the hardness of the rank syndrome decoding (RSD) problem and the efficient decoding algorithm of their concatenation.

This paper is organized as follows : Section 2 we introduce an overview on signature schemes and some definitions on the rank metric with the RSD problem. Then in section 3, we describe the suggested signature scheme based on the RSD problem with the desired concatenation code. The security analysis is studied in section 4. Finally, we conclude our work.

II. Preliminary

A. Overview on signatures schemes

Generally, all signatures schemes consist of three steps or more precisely algorithms:

- Generation of pair of keys : public and secret.
- Construction of the signature using a cryptosystem (MacEliece or Niederreiter) with the secret key and a hash function on message M.
- Verification of the signature if it is valid using the public key.

The conditions that every signature should achieve are as follows:

- Message authentication: The sender of the message is authentic.
- Integrity of the message: Message has not been modified during transmission.
- Non repudiation: The sender of a message can not deny the creation of the message.

B. Background on rank metric codes

Let $\mathbb{F}_q$ be a finite field of q elements and let $\mathbb{F}_{q^m}$ be an extension field of degree m. Let $x = (x_1, \ldots, x_n)$ be a vector over $\mathbb{F}_{q^m}$ and $(a_1, \ldots, a_m)$ be a basis of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$ such that $a_i \in \mathbb{F}_q$ for $i = \{1, \ldots, m\}$ and $x_j = \sum_{i=1}^{m} \alpha_{ij} a_i$ for $j = \{1, \ldots, n\}$.
The maximal number of elements x_j that are linearly independent over $\mathbb{F}_q$ define the **rank** of x over $\mathbb{F}_q$ which denoted by $rk(x|\mathbb{F}_q)$. **The rank distance** between two vectors x and y in $\mathbb{F}_{q^m}^n$ is : $d_r(x, y) = \mathtt{rank}(x - y|\mathbb{F}_q)$.

Any code C of length n and dimension k over $\mathbb{F}_{q^m}$ has a minimum rank distance $d_r(C) = d_r = min\{d_r(x, y)|x, y \in C, x \neq y\}$ is a rank metric code, verifying the Singleton bound $d \leq n - k + 1$. If this inequality is achieved the code will be a **Maximum rank distance (MRD) codes** for $m \geq n$. Therefore, we say that the code correct t errors if $t = \lfloor \frac{d-1}{2} \rfloor$.

The $k \times n$ generator matrix G of a MRD code is defined for any set of elements $g_1, \ldots, g_n$ from $\mathbb{F}_{q^m}$ that are linearly independent over $\mathbb{F}_q$ and its parity check matrix H which has for any elements from $\mathbb{F}_{q^m}$ linearly independents over $\mathbb{F}_q$ the following definition

$$G = \begin{bmatrix} g_1 & g_2 & \cdots & g_n \\ g_1^{[1]} & g_2^{[1]} & \cdots & g_n^{[1]} \\ \vdots & \vdots & \ddots & \vdots \\ g_1^{[k-1]} & g_2^{[k-1]} & \cdots & g_n^{[k-1]} \end{bmatrix} \quad (1)$$

and

$$H = \begin{bmatrix} h_1 & h_2 & \cdots & h_n \\ h_1^{[1]} & h_2^{[1]} & \cdots & h_n^{[1]} \\ \vdots & \vdots & \ddots & \vdots \\ h_1^{[d-2]} & h_2^{[d-2]} & \cdots & h_n^{[d-2]} \end{bmatrix} \quad (2)$$

where $g^{[i]} = g^{q^i \mod n}$ (respectively $h^{[j]} = h^{q^j \mod n}$) is the i-th Frobenius power of g with $i = 1 \ldots n$. (respectively the j-th Frobenius power of h with $j = 1 \ldots d-1$).

Definition 1: The $\mathbb{F}_q$-sub vector space of $\mathbb{F}_{q^m}$ generated by $\{g_1, \ldots, g_n\}$ denoted by E is the **support** of g of dimension r (where $r = \mathtt{rank}(g|\mathbb{F}_q)$).
The number of possible supports of length n and dimension r over $\mathbb{F}_{q^m}$ can be calculated by the Gaussian binomial $\begin{bmatrix} n \\ r \end{bmatrix}_q \sim (q^{rn})$. This notion is very interesting in the RSD problem to recover the complete coordinates of g.

In the sequel, we define two known codes in order to construct another one to analyze our application to cryptography.
Gaborit et al. [9] proposed a new codes that are analogy to the LDPC codes as given in the following definition:

Definition 2: The **LRPC codes** of rank d, length n and dimension k over $\mathbb{F}_{q^m}$, has $H(h_{i,j})$ as a $(n-k) \times n$ parity-check matrix of weight d which represents the dimension of F the subspace of $\mathbb{F}_{q^m}$ generated by coefficients of H, ie: we write $h_{i,j} = \sum_{l=1}^{d} h_{i,j,l} F_l$. Where $\{F_1, \ldots, F_d\}$ form a basis of F.
Recently, a new code had been proposed by Terry et al. [2] defined in the rank metric in analogy to the Generalized Reed-Slomone codes. A definition of such codes is given as follows:

Definition 3: (λ-Gabidulin codes [2]) Let $g = (g_1, \ldots, g_n) \in \mathbb{F}_{q^m}^n$ be linearly independent over $\mathbb{F}_q$ and $\lambda = (\lambda_1, \ldots, \lambda_n) \in \mathbb{F}_{q^m}^n$. The λ-Gabidlin code over $\mathbb{F}_{q^m}$ of dimension k associated with vector g and λ is the code generated by a matrix G_λ of the form

$$G_\lambda = \begin{bmatrix} \lambda_1 g_1 & \lambda_2 g_2 & \cdots & \lambda_n g_n \\ \lambda_1 g_1^{[1]} & \lambda_2 g_2^{[1]} & \cdots & \lambda_n g_n^{[1]} \\ \vdots & \vdots & \ddots & \vdots \\ \lambda_1 g_1^{[k-1]} & \lambda_2 g_2^{[k-1]} & \cdots & \lambda_n g_n^{[k-1]} \end{bmatrix} \quad (3)$$

and its parity check matrix is given by

$$H_\lambda = \begin{bmatrix} \lambda_1^{-1} h_1 & \lambda_2^{-1} h_2 & \cdots & \lambda_n^{-1} h_n \\ \lambda_1^{-1} h_1^{[1]} & \lambda_2^{-1} h_2^{[1]} & \cdots & \lambda_n^{-1} h_n^{[1]} \\ \vdots & \vdots & \ddots & \vdots \\ \lambda_1^{-1} h_1^{[n-k-1]} & \lambda_2^{-1} h_2^{[n-k-1]} & \ldots & \lambda_n^{-1} h_n^{[n-k-1]} \end{bmatrix} \quad (4)$$

Such codes had been selected in the application of cryptography; the McEliece like cryptosystem and proved out that it can be resistant for the rank syndrome decoding

problem (RSD) to known attacks for well chosen parameters.

The Rank Syndrome Decoding problem (RSD) was the most interesting problem studied for more than 20 years ago, to find the codeword x which satisfies the two conditions: $\texttt{rank}(x|\mathbb{F}_q) = r$ and $Hx^t = s$, with a given integer r, $s \in \mathbb{F}_{q^m}^k$ and H is a $(n-k) \times n$ matrix over $\mathbb{F}_{q^m}$ with $k < n$. This problem is NP-hard with a randomized reduction in [5] and is proved to be hard in [7] which is convenient for decoding algorithm security.

Proposition 1: Let C_1 and C_2 be a $[n, k_1, d_2]$ LRPC code and a $[n, k_2, d_2]$ λ-Gabidulin code respectively. The concatenation of these two codes is defined as a code $C = (C_1|C_2)$, with parameters $[n = n_1 \cdot n_2, k = k_1 \cdot k_2, d]$ where $d \geq d_1 \cdot d_2$. The code C consists of vectors $v = (v_1, v_2)$ where $v_1 \in C_1$ and $v_2 = \lambda v_1 \in C_2$ with $\lambda \in \mathbb{F}_{q^m}^n$.

This construction increases all the parameters of the code and its decoding algorithm will consider first the decoding algorithm D_1 [7] of the LRPC code C_1 as the inner code and then the decoding algorithm D_2 [2] of the λ-Gabidulin C_2 as the outer code. Such decoding algorithm is an error/erasure decoder which can correct r errors and r' erasures only when $2r + r' < d$.

III. New rank signature scheme

For the construction of the scheme, we define the subspace $E = E' + T$ of dimension $t = 2r + r'$ over $\mathbb{F}_{q^m}$ such that E' is the subspace of errors of dimension $2r$ and $T \subset E'$ is the subspace of erasures of dimension r'.

*a) **Key generation**:*

- **Input**
  - Invertible matrix S of order $(n-k)$ over $\mathbb{F}_{q^m}$.
  - Invertible matrix P of order $(n + r')$ over $\mathbb{F}_{q^m}$ as given in [4].
  - A concatenated code over $\mathbb{F}_{q^m}$ between LRPC and λ-Gabidulin code with parity check matrix H of size $(n-k) \times n$. Which can decode t errors.

  Choose at random a matrix R of size $(n-k) \times r'$ and compute $H_{pub} = S[H|R]P$.
- **Output :** A pair of keys (pk, sk) such that
  - pk: H_{pub}, hash function $\texttt{hash}$ and an integer l.
  - sk: S, P, H and R with D_1 and D_2.

*b) **Signature of message** M:*

- **Input :** A message M and sk.
  1) Pick randomly $b \in \{0,1\}^l$.
  2) Choose r' random independent elements $(e_1, \ldots, e_{r'}) = e$ of $\mathbb{F}_{q^m}$.
  3) Compute $h = \texttt{hash}(M|b)$.
  4) Decode $h' = S^{-1}h^\top - Re^\top$ by the decoding algorithms D_1 and then by D_2.
  5) If the decoding algorithm works and outputs $e' = (e_{r'+1}, \ldots, e_{n+r'})$ with $\texttt{rank}(e'|\mathbb{F}_{\shortparallel}) = 2r+r'$ then the signature outputs $\sigma(e''(P^\top)^{-1}, b)$ where $e'' = (e_1, \ldots, e_{n+r'})$. Else return step 1.
- **Output :** The signature $\sigma = (e''(P^\top)^{-1}, b)$.

*c) **Verifying of validity**:*

- **Input :** pk and σ.
  1) Check if $\texttt{rank}(e'') \leq t$.
  2) Check if $H_{pub}e''^\top = h$ then $h = \texttt{hash}(M|b)$.
- **Output :** "Valid" if $H_{pub}e''^\top = \texttt{hash}(M|b)$, else "Invalid".

After generating the pair of keys, the signer initialized small vector b over $\mathbb{F}_q$ in order to compute it with the hash of the message M, and choose randomly a vector $(e_1, \ldots, e_{r'}) = e$ in a random support T over $\mathbb{F}_{q^m}$. Then, the signer decode the hash value by performing the decoding algorithm of the dual matrix of the public code using D_1 and D_2 with t errors. If such decoding returned to give $(e_1, \ldots, e_n)$ of rank weight $t = 2r + r'$ then the signature will be transmitted to the verifier as a couple of $(e''(P^\top)^{-1})$ with $e'' = (e_1, \ldots, e_{n+t_1})$ which will assure that the number of errors/erasures is exactly t and that the $H_{pub}e'^\top = \texttt{hash}(M|b)$. If the decoding does not work or even the verification was not valid then it will outputs "Invalid", else output will be "Valid".
Since this signature presents a variant of the RankSign [2] we set the complexity of the signature and the verification algorithm about $(n-k)(n+r')\log_2(q)$ and the public key size of about $(n-k)(k+r')m\log_2(q)$ while the signature size equal to $(m+n+r')t\log_2(q)$.

Correctness of the scheme

To ensure the correctness of the signature we check the decoding capability of e''^{-1} and the output $e' = (e'_1, \ldots, e'_{n+r'})$. Hence, we decode first by $D_1 : D_1(h') = C(h'')$ then by $D_2 : D_2(h'') = e'$ for an output e' of rank weight less than or equal to t and the verifier should obtain $H_{pub}e''^\top = H_{pub}h'^\top = H_{pub}(S^{-1}h - Re'^\top)^\top = e'$. We can write : $H_{pub}e''^\top = h \Rightarrow [R|H]Pe^\top = S^{-1}h^\top \Rightarrow [HP_1e'^\top|RP_2e^\top] = S^{-1}h^\top$ where P_1 and P_2 are sub-blocks of P. By applying the decoding algorithm we get the output of decoding for $S^{-1}h^\top - RP_2e'^\top$ which is e'. Therefore, we can decode correctly only when the rank weight of e'' and $S^{-1}h - Re'^\top$ is less or equal to the decoding capability t.

IV. Security Analysis

The security of this signature algorithm is based on the difficulty of RSD problem, it can benefits from such a problem to withstand existed attack. Which has been developed over the years and categorized as attacks; on the PKC like the *message recover* which used the decoding attack and like the *public key recover* which used the algebraic attack. Rather than this, they used the attacks of Rank Syndrome Decoding problem and classified into combinatorial and algebraic attacks. Attacks on the message like the *information set decoding* which was developed in 1962 by Prang [10] as a technique of direct attack on the message. It is enough to find a set of k information positions with no errors. In the rank

metric, it has been converted into the error support attack [8]. Another type which attack directly on the signature like the forgery attack which also proposed to forge the real signature algorithm and consists in generating the valid signature of a message M that has not been signed by the right person.

The proposed signature has the property of mixing two interested codes from the rank metric. The application of the LRPC codes had a moderate public key size. While the λ-Gabidulin code had for chosen parameters a fast run time and resistant to Overbeck attack [15] and [16], [17].
In the attack of Debriz et al. [17], it was given a particular case for which their attack can't be feasible on RankSign [7]; if the minimum distance of the public code is not too small ($d \geq 3$) and $(n-k)d$ is not too close too n. Roughly speaking, this attack can be feasible when it is provided 3 condition naturally given by the RankSign; $m = (r - t')(d + 1)$, $n - k = d(r - t - t')$ and $n = (n - k)d$ with t' is the dimension of subspace T' for which the attacker choose the matrix H' for decoding algorithm. With respect to this conditions we choose parameters to withstand such an attack.

The table I we suggest a set of parameters for LRPC [7] and λ-Gabidulin [2]. Their public key sizes (bits) with a moderate public key size of their concatenation.

TABLE I
PUBLIC KEY SIZES WITH SECURITY LEVEL 120.

Type of code $[n, m, k, q, t, r', r]$	Public key size
$[16, 18, 8, 2^{16}, 2, 4, 6]$ LRPC [7]	23040
$[79, 83, 31, 2, 8 = a]$ λ-Gab [2]	15430
$[1264, 83, 248, 2, 48, 8, 20]$ Concatenation	21587968

In the table below II we compare the sizes of signature, secret key and public key with our variant in security level 128. Our variant has larger public key size and secret key size while it is moderate in the signature size.

TABLE II
COMPARISON OF SIZES OF OUR CASE WITH RANKSIGN, RANK VERON AND RANK CVE SIGNATURE IN SECURITY LEVEL 128.

SIGNATURE Scheme (parameters)	$\|sign\|$	$\|sk\|$	$\|pk\|$
RankSign [7]$(n, n-k, m, q, t, r, r')$ $(16, 8, 18, 2^{16}, 2, 4, 6)$	3456	41472	23040
Rank Veron [14] $(q, m, n, k, r, \sigma, h)$ $(2, 80, 64, 30, 9, 219, 256)$	1719296	7520	77124
Rank CVE [14]$(q, m, n, k, r, \sigma, h)$ $(2, 80, 64, 30, 9, 128, 256)$	27389952	5120	310084
Concatenation (n, m, k, q, t, r', r) $[1264, 83, 248, 2, 48, 8, 20]$	65040	107265216	21587968

V. CONCLUSION

We proposed a concatenation code from LRPC and λ-Gabidulin codes and gave new version of RankSign: signature algorithm which had a moderate public key size and signature size with a considerably high level security. The art of having an efficient and fast signature scheme is an attractive subject to study in the future work.

VI. ACKNOWLEDGMENTS

Sedat Akleylek was partially supported by TUBITAK under grant no. EEEAG-117E636.

REFERENCES

[1] NIST Post-quantum cryptography standardization website https://csrc.nist.gov/Projects/Post-Quantum-Cryptography/Round-1-Submissions
[2] Terry S-C-L and H-T. Chik, "A new Gabidulin-like code and its application in cryptography". accepted paper to the C2IS Conference 2019.
[3] N. Courtois, M. Finiasz and N. Sendrier, "How to achieve a McEliece based digital signature scheme", Proc. of Asiacrypt 2001, Springer LNCS Vol. 2248, pp. 157-174, 2001.
[4] E.M. Gabidulin, "Attacks and counter-attacks on GPT public key cryptosystem". Designs, Codes and Cryptography, pp. 171-177, 2008.
[5] P. Gaborit and G. Zémor, "On the hardness of the decoding and the minimum distance problems for rank codes". submitted to CCC. 2014.
[6] P. Gaborit, O. Ruatta, J. Schrek and G. Zémor, "Rank based cryptography : a credible post-quantum alternative to classical". Post - Quantum World. 2015.
[7] P. Gaborit, O. Ruatta, J. Schrek and G. Zémor, "RankSign: An Efficient Signature Algorithm Based on the Rank Metric", PQCrypto 2014: 88-107, 2014.
[8] P. Gaborit, O. Ruatta and J. Schrek, "On the complexity of the rank syndrome decoding problem", eprint. http://arxiv.org/abs/1301.1026, 2013.
[9] P. Gaborit, G. Murat, O. Ruatta and G. Zmor, "Low Rank Parity Check Codes and their application in cryptography", Published in Workshop Codes and Cryptography (WCC 2013), Bergen (available athttp://www.selmer.uib.no/WCC2013/pdfs/Gaborit.pdf), 2013.
[10] E. Prange, "The Use of Information Sets in Decoding Cyclic Codes", IRE Trans.Inform. Theory 8(5), p.p. 5-9, 1962.
[11] J. Stern, "A new paradigm for public key identification". IEEE Transactions on Information Theory, IT 42(6), pp. 2757-2768. 1996.
[12] P. Santini, M. Baldi, G. Cancellieri and F. Chiaraluce, "Hindering reaction attacks by using monomial codes in the McEliece cryptosystem",https://arxiv.org/abs/1805.04722, 2018.
[13] K. Jon-Lark, K Young-Sik, G. Lucky, J.K. Myeong and L. Nari, "McNie: A code-based public key cryptosystem", https://arxiv.org/abs/1812.05008, 2018.
[14] E. Bellini F. Caullery1, A. Hasikos, M. Manzano1, and V. Mateu, "Code-based signature schemes from Identification protocols in the rank metric", International Conference on Cryptology and Network Security, CANS 2018: Cryptology and Network Security pp 277-298, 2018.
[15] R. Overbeck, "Structural attacks for public key cryptosystems based on Gabidulin codes", Journal of Cryptology 21(2):280-301, 2008.
[16] A. Horlemann-Trautmann, K. Marshall and J. Rosenthal, "Considerations for Rank-based Cryptosystems", In IEEE International Symposium on Information Theory (ISIT 2016), pp. 2544-2548.
[17] A. Otmani, H. T. Kalachi and S. Ndjeya, "Improved Cryptanalysis of Rank Metric Schemes Based on Gabidulin Codes". Designs, Codes and Cryptography 86(9):1983-1996, 2018.
[18] T. Debris-Alazard and J.P. Tillich, "An attack on a NIST proposal: RankSign, a codebased signature in rank metric", arXiv preprint arXiv: 1804.02556, 2018.

Encrypting the TCM Encoder with Locally Rotated Constellations in Rayleigh Fading Channel

Rekkal kahina
Department of Electrical Engineering, Faculty of Technology,
Tahri Mohammed University-Bechar
Bechar, Algeria

Abdesselam Bassou
Department of Electrical Engineering, Faculty of Technology,
Tahri Mohammed University-Bechar
Bechar, Algeria

Rekkal Sarah
LAPECI Laboratory
University of Oran 1 Ahmed Ben Bella;
Oran, Algeria

***Abstract*---- Digital wireless communication over fading channels is hardly possible without using some kind of error protection or channel coding. To this end, in this paper, we propose to use Trellis Coded Modulation (TCM) encoder joined with Locally-Rotated (LR) constellations protected by Rivest–Shamir–Adleman (RSA) Algorithm which is asymmetric cryptography algorithm. Simulation results over Rayleigh fading show the performance gain of TCM and LR 8PSK joined by RSA cryptosystem compared to the original TCM 8 PSK and TCM with LR 8 PSK.**

***Keywords— TCM+LR 8PSK , Rayleigh fading channel, Wireless communication, RSA Algorithm,* Securing the transmission.**

I. INTRODUCTION

Wireless communications continue to attract the attention of both the research community and industry. In 1990, a mobile telephone was still quite expensive, whereas today most teenagers have one, and they use it not only for calls but also for data transmission. More and more computers use wireless local area networks (WLANs), and audio and television broadcasting has become digital. One of the most important challenges for communications engineers is to design optimal systems that can protect transmitted messages from channel errors. Shannon's capacity theorem (Forney and al. **[1])** proves that it is theoretically possible to achieve reliability in the transmission of an information sequence throughout a linear Gaussian channel by using coding. Many of the above-mentioned communication systems make use of sophisticated techniques that are known as Trellis Coded Modulation (TCM) and The RSA algorithm.

The first, TCM is a joint coding and modulation technique for digital transmission proposed by Ungerboeck in 1982 **[2]**, it has become very popular during recent years because of its theoretical foundations as well as its numerous applications, spanning high-rate digital transmission over voice circuits, digital microwave radio relay links, and satellite communications. In essence, it is a technique to obtain significant coding gains (3-6 dB) sacrificing neither data rate nor bandwidth and they can be decoded with the Viterbi or the Bahl–Jelinek (symbol-by-symbol Maximum a Posteriori 'MAP') algorithm (Bahl and al. **[3]).** In 1981 (Divsalar and al.) **[4]** designed the signal constellations to be asymmetric which obtain a performance gain over the traditional symmetric constellations combined with trellis coding.

The simulation results in (Rekkal and al. **[5])** have shown that the TCM+LR-UGM outperforms the TCM+LR Ungerboeck mapping by a gain of 2.5 dB and by a gain of 5 dB compared to the 8 state TCM+LR.

Trellis-coded modulation with Ungerboeck-Gray mapping (TCM-UGM) is more reliable over Rayleigh fading channel due to the mapping technique that combine both Ungerboeck mapping and Gray code mapping This TCM-UGM code outperform the performance of Ungerboeck TCM code by 0.26 dB over Gaussian channel and 2.59 dB over Rayleigh fading channel at BER = 10^{-5}**.[6].**

The second, The RSA cryptosystem is an example of a "public key" system. This means that everyone can know the encryption key, but it is computationally infeasible for an unauthorized person to deduce the corresponding decryption key.

The system includes a communications channel coupled to at least one terminal having an encoding device and to at least one terminal having a decoding device. A message-to-betransferred is enciphered to ciphertext at the encoding terminal by encoding the message as a number M in a predetermined set. That number is then raised to a first predetermined power (associated with the intended receiver) and finally computed. The remainder or residue, C, is... computed when the exponentiated number is divided by the product of two predetermined prime numbers (associated with the intended receiver).

The rest of this article is organized as follows: In section II, we present channel coding TCM encoder used in wireless communication systems which often have to cope with severe multipath fading in a mobile radio channel and we

propose to join it with new technique of modulation that improves trellis-coded modulation performance. This technique called locally-rotated constellations based on gathering the modulation constellation points into symmetric subsets and rotating these subsets by an optimum angle proposed by (Rekkal and Bassou [5]). Moreover, we use, the mapping techniques which combine both Ungerboeck mapping and Gray code mapping the results called TCM+LR-UGM. In section III we will briefly review RSA algorithm. Section IV introduces our implementation method which we join the TCM+LR with the RSA cryptosystem which takes great computational cost. In many RSA applications, user uses a small public key to speed up the encryption operation. However, the decryption operation has to take more computational cost to perform modular exponentiation by this case.Section V analyzes the simulation results. Finally, we make some conclusions in section VI.

II. TRELLIS CODED MODULATION WITH LOCALLY-ROTATED (LR) CONSTELLATIONS

The key idea of TCM schemes is that modulation and coding are combined in order to map the information bits to a modulated constellation signal set. The error correcting code mainly used is the (m/m+1) rate Trellis code or convolutional code, as example we present 8-state rate, 2/3 TCM encoder shown in figure 1.

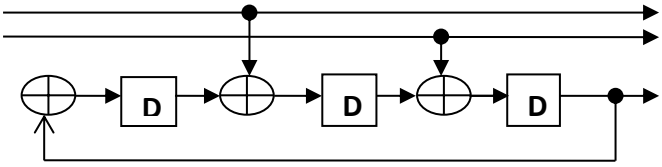


Fig. 1 Example of an 8-state TCM encoder [2].

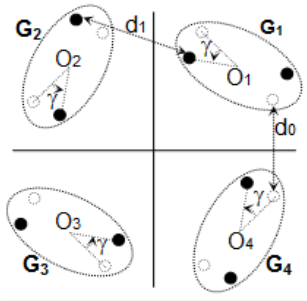


Fig. 2 Symmetric and Locally-Rotated (LR) constellations of 8PSK.

The TCM encoder of Figure 1 has three polynomials expressed as: $H_0(D) = D^3+1$; $H_1(D) = D$; $H_2(D) = D^2$, and the code generator is ($h0 = 1001_2 = 11_8$, $h1 = 0010_2 = 02_8$, $h2 = 0100_2 = 04_8$).

The 8 PSK constellation used according to the TCM encoder (shown in Fig.1) is presented in figure 3.

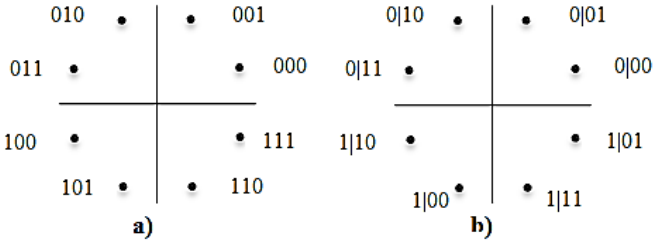


Fig. 3 a) Example of Symmetric constellations 8 PSK using Ungerboeck mapping; **b)** Example of Symmetric constellations 8 PSK using Ungerboeck Gray mapping.

The minimum Euclidean distance of symmetric constellation represented in white circles which equal to **0.765**.

1. Now we describe the construction of the proposed approach of locally-rotated LR-MPSK constellation.

Symmetric and locally-rotated 8PSK constellations are presented in Fig. 3 (symmetric constellation is represented by the white circles and the asymmetric (locally-rotated) by the black circles). The optimum value of the rotation angle (γ) is reached, according to the coordinates (d, d) of the center of group G_1, when the Euclidean distance d_1 given by

$$d_1 = 2\sqrt{d^2 - \frac{1}{\sqrt{2}} d d_0 \cos\gamma + \frac{1}{8} d_0^2} \qquad \textbf{(1)}$$

equals the minimum Euclidean distance d_0 .

We conclude that the rotation angle (γ) around the center O_i ($i \in \{1, \ldots, 4\}$) of the two point group G_i is optimal when the line that passes over the two points cross the center O_{i+1} of the group G_{i+1}. Thus, the optimum angle is $\gamma_{op} = \frac{\pi}{4}$ in the case of LR 8PSK.

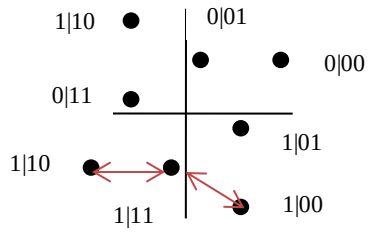


Fig. 4 Locally-Rotated (LR) constellations with Ungerboeck-Gray mapping of 8PSK.

A straight line distance between any two points is called the Euclidean distance. For a point p1 at (x1, y1) and another point p2 at (x2, y2), the Euclidean distance is given by the familiar formula:

$$\sqrt{(x_1 - x_2)^2 + (y_1 - y_2)^2} \quad \textbf{(2)}$$

The Minimum Euclidean Distance between two adjacent black circles of the LR-8PSK equal to **0.919** is greater than 0.765.

III. THE RSA ALGORITHM

Cryptography is the encryption of text in such a manner that outsiders to the code cannot understand the code, but the desired reader is able to decrypt the encryption so as to understand the message.

RSA is one of the first practicable public-key cryptosystems and is widely used for many applications including secure data transmission, virtual private networks, electronic commerce and secure internet access. RSA is widely used for digital signature and digital envelope, which provide privacy and authentication.

RSA stands for Ron Rivest, Adi Shamir and Leonard Adleman, who first publicly described the algorithm in 1977. Clifford Cocks, an English mathematician, had developed an equivalent system in 1973, but it wasn't declassified until 1997. [7].

The keys for the RSA algorithm are generated the following way:

1. Choose two distinct prime numbers p and q and denote $n = p.q$.
2. Compute $\varphi(n) = (p-1)(q-1)$ where φ is Euler's totient function.
3. Choose a large integer d such that $1 < d < \varphi(n)$ and $gcd\,(d, \varphi(n)) = 1$; i.e., e and $\varphi(n)$ are coprime.
4. Determine e as $e \equiv d - 1 (mod\ \varphi(n))$; i.e., e is the multiplicative inverse of d $(modulo\ \varphi(n))$.
5. Encryption: Given a message w satisfying $w < n$, then the cryptotext $c = w^e\ mod\ n$.
6. Decryption: plaintext $w = c^{\,d} mod\ n$.

IV. TCM+LR WITH THE RSA CRYPTOSYSTEM

The security of the transmission chain becomes more and more necessary with the evolution of communications in terms of the number of users and the nature of the information to be transmitted. During these years, the researches were pushed towards the improvement of the quality of the information received as well as the robustness of the algorithms which treat this transmitted information. For this, currently any high-performance telecommunication system requires a robust encryption system to protect against possible attacks.

In this paper, we study the possibility of using the RSA algorithm, based on its different properties and its specific behavior, to encrypt the information in a secure transmission. We test the security of this method by applying a plaintext attack chosen as a tool for breaking the encryption system.

The RSA algorithm can be inserted in a communication channel can be represented as illustrated in Figure 7.

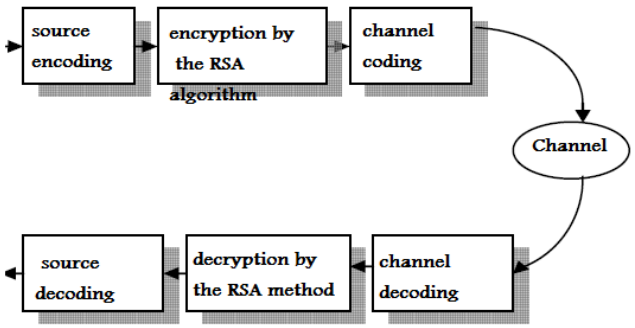


Fig.7 Chain of transmission of an encrypted message by RSA algorithm.

Attacking techniques are used to break the algorithm and recover the complaints without having access to the key. Indeed, the intruder knows exactly the design of the algorithm and the operation of the encryption system to study, that is to say, he knows everything about the subject except the secret keys.
This is an obvious condition in secure communications today.
However, history has proven that maintaining the secrecy of the encryption system is very difficult.

In our work we used the type chosen for the clear text attack:
As an example of how to produce the keystream, we use a 2 symbol source, $S_2 = \{s_1, s_2\}$ and we ask for the ciphertext of messages built only by s1 or s2, assuming that if ($i \in \{1, 2\}$) is the symbol corresponding to each useful sub-interval and x the reiterated which visits the forbidden intervals.
Under these conditions, we conduct a selected plaintext attack, requesting the encrypted text of the message in clear following: P = ($s_1\ s_1\ s_1\ s_1\ s_1\ s_1\ s_1\ s_1\ s_1\ s_1\ s_1\ s_1 \ldots$).
If we obtain for example the corresponding ciphertext C = (5 3 2 2 2 3 2 3 2 2 3 2 ...), we can be sure that the 6th symbol in the keystream is s1, the 9th symbol is also s1, as well as the 11th and so on. After considering the whole message, we get a partial knowledge of the keystream:
K=x x x x x s_1 x x s_1 x s_1 x s_1 x s_1 x x s_1 x s_1 x x s_1 x s_1 x s_1 x x s_1 x s_1....

If we use all the attractor [0, 1] instead of a portion [0.2, 0.8], we can ensure that the letters marked x must be s2 (except for the first x which corresponds to the initial condition). But since it is only one part of the interval, they can correspond to an iteration lower than the terminal 0.2 or superior to the terminal 0.8.

Then we ask for the encrypted text of the plain text message: P = (s2 s2 s2 s2 s2 s2 s2 s2 s2 ...).

If we get C = (1 2 3 9 5 7 5 1 1 1 ...), as quoted before, we can conclude that the letters that correspond to the position in the sequence indicated by the number of iterations in the encrypted message represent s2. We are adding this information to the first Keystream sequence and we will have:

K = xs2xs2xs1s2xs1xs1xs1xs1s2xs1xs1s2xs1 xs1xs1s2xs1 xs1s2 ...

Now, we are certain that the letter x corresponds to an iteration outside the interval [0.2, 0.8], except the first letter x which corresponds to the initial condition.

By following this calculation method, which requires only 2 selected plaintext texts, we get all the keystream. To obtain a longer key, we simply need to request the encrypted message of a long plaintext. It is obvious that any message encrypted by the same values of x0 and b use the same keystream, which depends only on the parameter b and the initial condition x0, so it can be easily broken by cryptanalysis. We can then generalize this method to higher order sources.

The reason why the symbol x appears frequently in the keystream is easy to understand by looking at Figure 3 which gives the invariant natural density of equation (1); since the regions near the extremities are visited with a high frequency. As a consequence of the choice of the interval [0 .2, 0.8], half of the iterations is neglected.

V.SIMULATION RESULTS

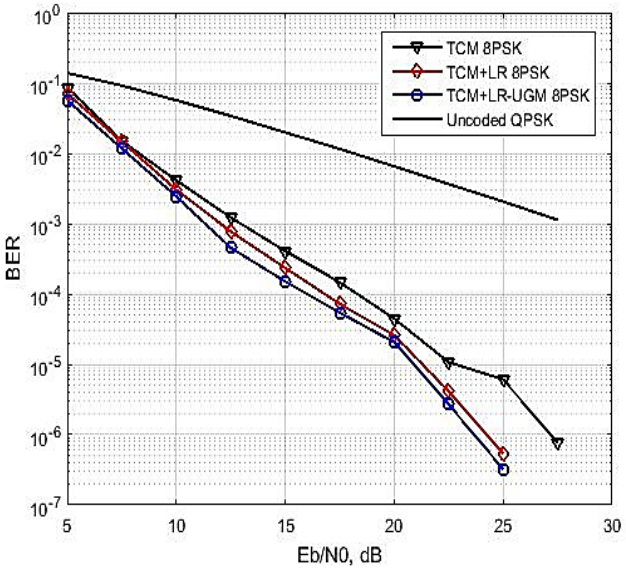


Fig.8 Comparison between with 8 states of TCM, TCM+LR and TCM+LR-UGM 8PSK over Rayleigh fading channel.

- In Fig.8, shows that with 3 memories, we get a slight improvement using TCM + LR-UG mapping compared to the TCM+LR but we obtain gain of 2.5 dB (approx.) compared to TCM-Sym Ungerboeck at BER = 10^{-6} over Rayleigh fading channel.

VI. CONCLUSION

In this work, the performance comparison of the variant of 8PSK+LR constellation TCM encrypted by RSA algorithm in wireless communication, 8PSK+LR constellation TCM and original 8PSK TCM was presented for spectral efficiency of 2bits/s/Hz over Rayleigh fading channel. The simulation results over Rayleigh fading channel shows that 8PSK+LR constellation TCM encrypted by RSA algorithm outperforms 8PSK+LR constellation TCM by gain of 2.5 dB at the BER= 10^{-5} and the gain of 7.5dB (approx.) compared the original TCM.

We concluded according to the simulation results that the proposed techniques based on 8PSK and LR constellation TCM encrypted by RSA algorithm signals are very vulnerable to channel fading compared to the others schemes.

References

[1] G. D. Forney Jr., R. G. Gallager, G. R. Lang, F. M. Longstaff, and S. U. Qureshi, "Efficient Modulation for Band-Limited Channels," IEEE J. Select. Areas in Commun., vol. JSAC-2, no. 5, pp. 632-647, Sep. 1984.

[2] G. Ungerboeck, 'Channel coding with multilevel/phase signals', IEEE Transactions on Information Theory, vol. 28, no. 1, pp. 55-67, 1982.

[3] L. Bahl, J. Cocke, F. Jelinek, and J. Raviv, "Optimal decoding of linear codes for minimizing symbol error rate," IEEE Trans. Inform. Theory, vol. IT-20, pp. 284–287, Mar. 1974.

[4] D. DIVSALAR, M. K. SIMON, and J. H. YUEN 'trellis coding with asymmetric modulations,' IEEE transactions on communications, vol. Com-35, no. 2, February 1981.

[5] Rekkal K., A Bassou, " Improving the Performance of Trellis Coded Modulation over Rayleigh Fading Channel Using Locally Rotated constellations", International Journal on Communications Antenna and Propagation (IRECAP), Vol.8, No. 1 February 2018.

[6] A. Bassou and A. Djebbari, "Contribution to the Improvement of the Performance of Trellis-Coded Modulation," WSEAS Transactions on Communications, Vol. 6, No. 2, pp. 307-311, February 2006.

[7] R. Hwang and C. Yao "An efficient decryption method for RSA cryptosystem",Conference Paper · April 2005
DOI: 10.1109/AINA.2005.97 · Source: IEEE Xplore.

Secure MD4 Hash Function Using Henon Map

Amine Zellagui
dept of electronic,University of Sciences and Technology of Oran
laboratory of coding and security of information LACOSI
Oran, Algeria
Email : amineget29@gmail.com

Naima Hadj-Said
dept of computer science,University of Sciences and Technology of Oran,
laboratory of coding and security of information LACOSI
Oran, Algeria
Email : nim_hadj@yahoo.fr

Adda Ali-Pacha
dept of electronic,University of Sciences and Technology of Oran
laboratory of coding and security of information LACOSI
Oran, Algeria
Email : a.alipacha@gmail.com

***Abstract*— Secure hash functions play a fundamental role in cryptographic and web applications. They are mainly used, in the context of digital signatures, to verify the integrity and authenticity of information, in recent years research have found weaknesses in a number of hash functions like MD4,MD5 and SHA-1 ,So in this paper a modified scheme of MD4 was proposed by replacing the original message index K and bit rotation S with new sequence using Henon chaos systems , this proposed scheme given high sensibility of any little change to the original message ,great statistical diffusion and confusion performance, high resistance to collision.**

Keywords— MD4 ,hash function ,chaotic maps ,Confusion and diffusion.

I. INTRODUCTION

the Internet has evolved so much that it has become an essential communication tool. However, this communication increasingly involves strategic issues related to the activity of companies on the Web. Transactions made through the network can be intercepted, especially since the laws are difficult to set up on the Internet, so we must ensure the security of this information, it is the cryptography that takes care of it.

The hash functions are used to calculate an arbitrary size input data with a fixed size fingerprint. This size generally varies between 128 and 512 bits. The traditional hash functions algorithms such as MD4 [1] , MD5 [2] , ripemd [3] and haval-127 [4] has been successfully attacked by X Wang in 2004 [5],and SHA-1[6] by Marc Stevens in 2017 [7], so,It encourages researchers to find alternatives to synthesis efficient hash functions with ease of computations.

in recent years ,the chaos systems has become most important by researchers [11] [12],which are known to be highly sensitive to initial conditions and control parameters and desired confusion and diffusion properties ,this properties has encouraged researchers to use chaos in crypto-systems and hash functions

in this paper, We propose a modification of the hash algorithms the most used of the MD family like MD4 by using a chaos systems ,to increase security, and make hash function more sensitive..

II. CHAOS SYSTEMS

Chaotic system is a dynamic deterministic system that has unpredictable behavior in the long run. This unpredictability is due to sensitivity to initial conditions and he has a periodic behavior.

A. Henon map

The Hénon map is a 2D chaotic map created by Michel hénon [8],it is a discrete-time dynamical system. The Hénon map takes a point (x_n, y_n) showed in fig 1, It is mathematically defined as :

$$x_{n+1} = 1 - ax_n^2 + y_n$$
$$y_{n+1} = bx_n$$

Where a=1.4,b=0.3.

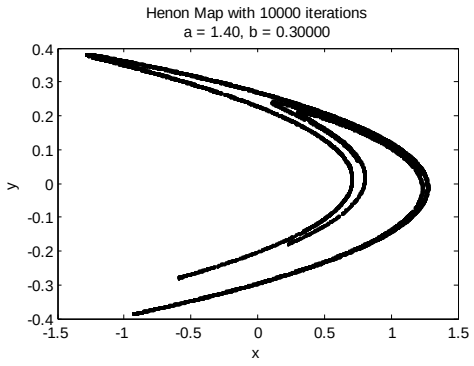


Fig. 1 Bifurcation diagrams of Hénon map

III. MD4 HASH FUNCTION

The MD4 algorithm considered as the origin of the MD-SHA family designed by Rivest in 1990, it is an iterative hash function running on 32-bit words. The round function takes as input a 4-word chaining variable and a 16-word message block and maps it to a new chaining variable. All operations are defined on 32-bit words. The transformation consists of 3 rounds, and each round consists of 16 steps [1].(see fig 2)

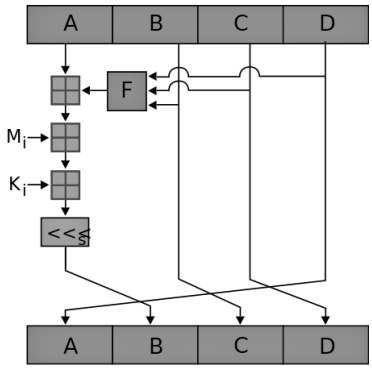


Fig. 2 An MD4 operation

Where k[i] is the message index , with : 0 ⩽k ⩽15, and S is the bit rotation on the left with 0 ⩽S ⩽15 .
There are three possible functions F; a different one is used in each round

- F (X, Y, Z) = XY v (-X) Z
- G (X, Y, Z) = XY v XZ v YZ
- H (X, Y, Z) = X + Y + Z

To calculate the message digest , we need to follow four step :

a) Padding : One bit "1" is appended to the message, then "0" bits are appended so that the length in bits of the padded message becomes congruent to 448, modulo 512.Now we add 64-bit to the result of the previous step,where 64-bits is the length of the message before the padding bits were added. the resulting message (after padding) has a length that is an exact multiple of 512 bits. Equivalently ,this message has a length that is an exact multiple of 16 (32-bit).

Example: Either the following message: 01100001 01100010 01100011 (in binary) ,length L = 24 bits

- Add '1' bit at the end of the message: 01100001 01100010 01100011 1 (the size becomes 25 bits)
- Then add '0' bits so that the bit length of the padded message becomes congruent to 448, module 512. (448-25 = 423 bits of zeros)
- 01100001 01100010 01100011 1 00 ... 0 (423 bits zeros to be added at the end, then the size becomes 448 bits).
- Now add 64 bits to the result of the previous step, take the original message size L = 24 in binary (24 => 00011000) + 56 bit of zeros

b) Initialize an Buffer: The main MD4 algorithm operates on a 128-bit state, divided into four 32-bit words, denoted A, B, C, and D. These registers are initialized to the following values :

- A = 67452301
- B = EFCDAB89
- C = 98BADCFE
- D = 10325376

Save A as AA, B as BB, C as CC, and D as DD.
AA = A ,BB = B ,CC = C ,DD = D

c) Process Message in 16-Word Blocks : The main algorithm then successively uses each 512-bit message block to change the state. The processing of a message block consists of three similar steps, called rounds; each round is composed of 16 similar operations based on a non-linear function F, a modular addition and a left rotation S.
Proceed as follows :
Algorithm:
for i = 0 à N / 15
for j = 0 to 15 do
set X[j] to M[i*16+j].
end

MD4 uses two "magic constants" in round two and three. The constant of round two is √2 and the constant of round 3 is √3. Here are their values in octal and hexadecimal (with high order numbers given first) [9]

- In Round 2 , constant (√2) : 013240474631(octal) , 5A827999 (hex)
- In Round 3 , constant (√3) : 015666365641(octal) , 6ED9EBA1(hex)

Let [A B C D K S] designate the operation :

Round 1 (0 ≤ j < 15): Let [A B C D i s] designate the operation

A = (A + F (B, C, D) + x [i]) <<< S.

Such as:
S = [3,7,11,19] rotation to the left, X is the 32 bit message with 0 ≤ i <16 (i in ascending mode)

Round 2 (16 ≤ j < 31): Let [A B C D i s] designate the operation

A = (A + G (B, C, D) + X [i] + 5A827999) <<< S.

Such as:
S = [3,5,9,13] rotation on the left and i = [0,4,8,12,1,5,9,13,2,6,10,14,3,7,11,15]

Round 3 (32 ≤ j < 47): Let [A B C D i s] designate the operation

A = (A + H (B, C, D) + x [i] + 6ED9EBA1) <<< S.

Such as:
S = [3,9,11,15] rotation to the left and i = [0,8,4,12,2,10,6,14,1,9,5,13,3,11,7,15]

d) Exit : The output message summary is A, B, C, D 128 bits in size, that is, we start with the byte of the

lower order of A and ends with the byte of the higher order of D, This completes the description of MD4.

IV. PROPOSED SCHEME OF MD4

To increase the security of MD4,and make it more sensitivity ,we will change the fixed values of K and S to the dynamic values by using Hénon map,

The procedure for producing the values of K and S is as follow :

Step 1 : Algorithm

- input : a,b,Ko,So,N>3000
- output : K,S
- Begin
- for i:= 1 to N do
- K(i+1) := (1-(a*K(1,i)^2) + S(1,i)*10^7)mod 16;
- S(i+1) := (b*K(1,i)*10^7) mod 32;
- End

Step 2 : take just The integer number of all values of K and S.

Step 3 : in each round ,Select 16 Number of K and 4 number of S , where ,In every number should not be repeated.

Example :

Round 1 : k=[1 16 12 6 13 11 9 15 2 7 8 3 5 4 10 14], S=[12 27 29 10] .

Round 2 : k=[10 1 9 13 2 6 4 16 5 7 8 11 12 14 15 3], S=[7 1 14 20] .

Round 3 : k=[4 1 9 8 2 6 5 7 11 12 13 14 15 10 16 3], S=[16 11 5 8] .

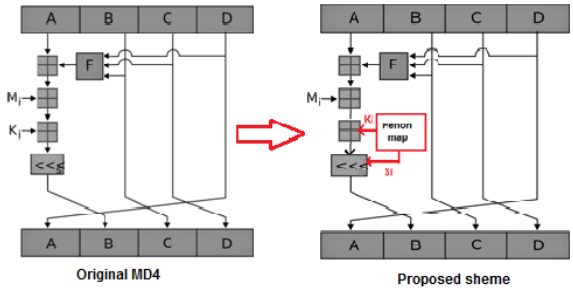


Fig .3 Proposed scheme of MD4.

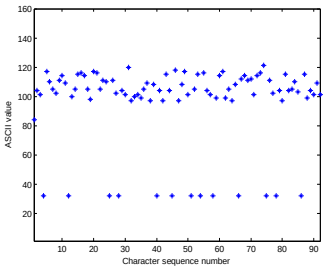
Note : if the block size of message superior of 512 bits (More block of length 512) ,we generate other value of K and S ,where Each number is different from the previous one and so

V. PERFORMANCE ANALISYS

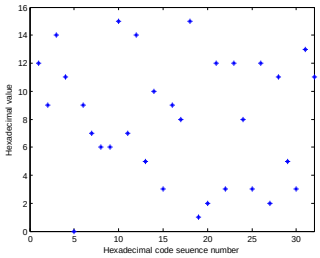
In this section, we perform several tests to determine the performance of our modified hash function. Performance is evaluated against the scan suite that includes hash distribution, message sensitivity, diffusion and confusion, collision resistance .we also provide a comparison with the original MD4.

The values assigned to initial conditions and parameters for simulation are: x0=0.02,y0=0.01,r=0.3,a=1.4.

A. Distribution Analysis : The uniform distribution of hexadecimal hash value is the crucial property of hashing scheme, we generate a message with random characters , then transformed to ASCII decimal codes plotted in fig 4 a), the hash values of the hashing scheme are uniformly spread over the possible range of hash values as illustrated in fig 4 b), This ensures that hash distribution is well uniform enough to hide information and act as a strong security measure



a)



b)

Fig. 4 a) random of message characters , b) hash value with proposed scheme of MD4.

B. Sensitivity to Small Changes in Message and Initial Conditions : in this subsection , we demonstrate the the high sensitivity of the proposed scheme of MD4 hashing function to small changes in original messages and initial conditions. The simulation for sensitivity is done under following conditions.

Condition 1: The original message is : « Secure hash functions play a fundamental role in cryptographic and web applications. »

Condition 2: Replace the first character of the original message "S" by "s"

Condition 3: Replace the last character of the original message "." by ":"

Condition 4: change x0=0.02 to 0.021.

Condition 5 : change y0=0.01 to 0.001.

-The corresponding 128-bit hash values in hexadecimal format are the following:

Condition1 : 08F8769488BE9823DE997EBEA21157DB

Condition 2: 069554335CC70CF3B90F8BC5F7915CBB

Condition 3: AE98822E37F373F748F4A5F11DF364B6
Condition 4: 0D069CCED560A6FFBAB7C7E7C68BB078
Condition 5: BCCDFEEFC5B9A11D128BC8B3E8603A35
All the hash value of proposed scheme with different conditions showed in fig 5

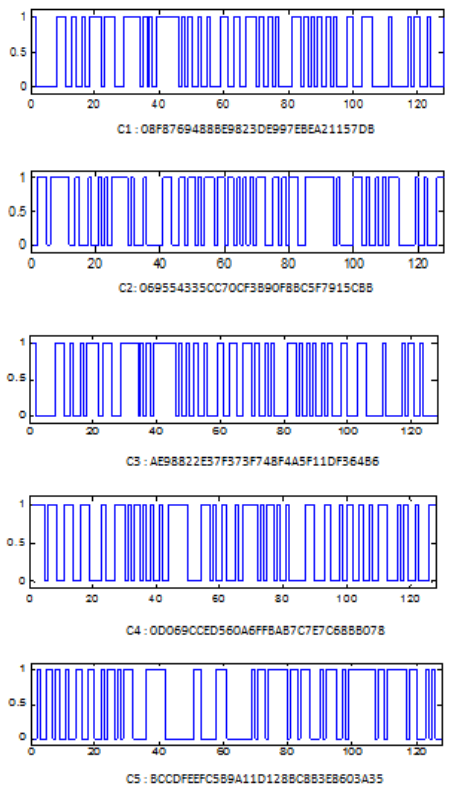


Fig.5 hash value of proposed scheme with different conditions.

the result of the binary representations of hash, demonstrate that a small modification in the message ,initial condition and control parameter can change all the hash value ,we can say that the proposed scheme has great sensitivity

C. *Statistic analysis of diffusion and confusion:* Due to security of hashing, Shannon developed two feature named Confusion and diffusion [10] to measure the performance of hashing algorithms and hide the message redundancy. any slight changes in original message should have 50% changing probability for each bit of hash value.
To perform statistical analysis of confusion and diffusion ,we need first to calculate the hash value of original message ,secondly we change 1 bit of original message and calculate hash value ,now the two hash values are then compared with each other in order to obtain the number of changed bits, this step will be repeated N times ,where N=256, 512,1024 and 10000.

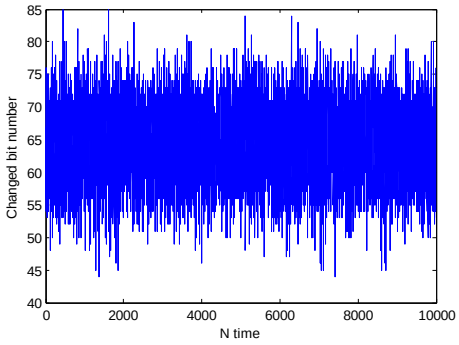


Fig.6 Spread of changed bit number.

The evaluation of diffusion and confusion capabilities is accounted through the following measures :

Minimum changed bit number :

$$B_{min} = \min(\{B_i\}_1^N)$$

Maximum changed bit number:

$$B_{max} = \max(\{B_i\}_1^N)$$

Mean changed bit number :

$$\bar{B} = \sum_{i=1}^{n} \frac{B_i}{N}$$

Mean changed probability :

$$P = \frac{\bar{B}}{128} \times 100\%$$

Standard variance of the changed bit number :

$$\Delta B = \sqrt{\frac{1}{N-1} \times \sum_{i=1}^{N} (B_i - \bar{B})}$$

Standard variance of probability :

$$\Delta P = \sqrt{\frac{1}{N-1} \times \sum_{i=1}^{N} \left(\frac{B_i}{128} - P\right)} \times 100\%$$

Table.1 Statistical outcomes for N = 256, 512,1024 and 10,000 of MD4

Parameter	256	512	1024	10000	Mean
B_{min}	45	45	45	42	44.25
B_{max}	80	80	83	84	81.75
$\bar{B}$	63.894	63.863	64.077	63.958	63.94
P%	49.917	49.893	50.010	49.967	49.94
ΔB	5.9433	5.7402	5.6240	5.6403	5.73
ΔP	4.6432	4.4845	4.3937	4.4065	4.48

Table.2 Statistical outcomes for N = 256, 512,1024 and 10,000 of Proposed sheme of MD4

Parameter	256	512	1024	10000	Mean
B_{min}	49	49	47	43	47
B_{max}	80	81	83	83	81.75
$\bar{B}$	64.039	64.095	64.230	63.954	64.08
P%	50.030	50.074	50.180	49.964	50.06
ΔB	5.4403	5.4045	5.6305	5.5960	5.51
ΔP	4.2502	4.2223	4.3988	4.3719	4.31

From the results in table 1 and 2, it can be observed that and P of proposed sheme are nearly the ideal values of n/2 and 50% respectively and better than original scheme. All values of ΔB and ΔP are very small, which signifies that diffusion and confusion capability of the proposed scheme is very strong and stable.

D. Resistance to collision attack : Collision resistance is a property of cryptographic hash functions ,a cryptographic hash function H is collision resistant if it is difficult to find two entries that give the same hash value, so in this subsection we test the Collision resistance of proposed scheme of MD4 by do the following :

we choose a message randomly and we get the hash value then stored in ASCII format ,Now We change and choose the one bit value in original message ,The two hashes with different messages are compared by counting the number of same ASCII characters at the same location.

$$d = \sum_{i=1}^{N} |t(e_i) - t(e_i')|$$

where :

e_i and e_i' are the ASCII characters at position i,d is the absolute difference and t is the thing that changing the ASCII code into corresponding decimal system value .the result are made in table 3.

Table. 3 Comparison on collision resistance for N=2048

Algo	min	max	mean	Mean/char
MD4	696	2322	1368	85.5322
Proposed sheme	538	2249	1371	85.7090

VI. CONCLUSION

In this article ,a new scheme of MD4 was proposed ,we changed fixed value of K and bit displacement S to dynamic value using chaotic Hénon map ,The chaotic maps provide high sensitivity to message and key such that even a little change results in dramatic changes in output hash.

This proposed scheme given high sensibility of any little change to the original message ,great statistical diffusion and confusion performance, high resistance to collision ,it can be considered as a keyed hash function by using initial value K0,S0 as a keys

the proposed scheme has simple structure and flexible ,so we can used in MD5 hash function and make it more sensitive.

REFERENCES

[1] Rivest R., 1992, "The MD4 Message-Digest Algorithm,"RFC 1320, MIT LCS and RSA Data Securit y, Inc

[2] Rivest R., 1992, "The MD5 Message-Digest Algorithm,"RFC 1321, MIT LCS and RSA Data Securit y, Inc

[3] Dobbertin H., Bosselaers A., Preneel B. (1996) RIPEMD-160: A strengthened version of RIPEMD, vol 1039. Springer, Berlin, Heidelberg

[4] Zheng, Y., Pieprzyk, J., Seberry, J.: HAVAL - A One-Way Hashing Algorithm with Variable Length of Output. In: ASIACRYPT 1992. LNCS, pp. 83–104. Springer, Heidelberg (1992)

[5] Wang, X., Feng, D., Lai, X., & Yu, H. (2004). Collisions for hash functions MD4, MD5, HAVAL-128 and RIPEMD.Cryptology ePrint Archive, report 2004/199

[6] D. Eastlake ,P. Jones,"US Secure Hash Algorithm 1 (SHA1)",RFC3174,September 2001

[7] Marc Stevens, Elie Bursztein, Pierre Karpman, Ange Albertini, Yarik Markov,The first collision for full SHA-1,CWI Amsterdam,Google Research 2017.

[8] M. Hénon (1976). "A two-dimensional mapping with a strange attractor". Communications in Mathematical Physics. 50 (1): 69–77.doi:10.1007/BF01608556.

[9] Addison-Wesley,The Art of Programming, Volume 2 (Seminumerical Algorithms), Second Edition (1981),Table 2, page 660.

[10] Shannon, C. E. (1949). Communication theory of secrecy systems. Bell Systems Technical Journal, 28, 656–715

[11] Musheer Ahmad . Shruti Khurana . Sushmita Singh . Hamed D. AlSharari. A Simple Secure Hash Function Scheme Using Multiple Chaotic Maps

[12] A. Kanso, H. Yahyaoui , M. Almulla,Keyed hash function based on a chaotic maps ,Information Sciences Volume 186, Issue 1, 1 March 2012, Pages 249-264

Using of Multi Chaotic System for Implementing a Good Cryptosystem

ALI CHERIF Khalfallah
Laboratory of coding and information security-LACOSI
University of Science and Technology of Oran - USTO-MB
Oran, Algeria
alicherif.kha@gmail.com
Khalfallah.alicherif@univ-usto.dz

HADJ SAID Naima
Laboratory of coding and information security-LACOSI
University of Science and Technology of Oran - USTO-MB
Oran, Algeria
naima.hadjsaid@univ-usto.dz

ALI PACHA Adda
Laboratory of coding and information security-LACOSI
University of Science and Technology of Oran - USTO-MB
Oran, Algeria
a.alipacha@gmail.com

Abstract—This article proposes an algorithm of confusion and diffusion of image encryption based on the logistic map and the attractor of Henon-Lozi. We chose the initial parameters of the logistic map and the Henon-Lozi Attractor as secret keys. The Henon-Lozi Attractor is used to generate a chaotic matrix to mask the pixel values and the logistic map uses to generate random sequences to make a permutation between the pixels.
The computer experience such as statistical analysis, sensitivity analysis proves that the proposed image encryption algorithm is robust and secure enough to be used in practice.

Keywords—Chaos, Encryption, Henon-Lozi, Attractor, Logistic map - P-box

I. INTRODUCTION

With the rapid growth of the image transmission requirement on the Internet, the protection of digital information from illegal uses is becoming increasingly important. Because of the large data capacity and the high correlation between pixels in image files, traditional techniques are not suitable for image encryption [1]. Compared to traditional methods (such as AES and DES), chaos-based image encryption schemes have shown superior performance [2-4].

The general permutation-diffusion procedure [5] for chaos-based image encryption consists of two steps: the diffusion and the permutation of the pixels. Fig. 1 illustrations its architecture. In the diffusion process, the pixel values are modified sequentially. In the permutation process, the position of the pixels in the image is changed, so that a tiny change for one pixel can extend to almost every pixel. of the entire image.

In this article, an image encryption method based on chaos is proposed. The key flow in the diffusion step generate by the Henon-Lozi function and combine with the pixel value of the image in clear, then the algorithm generates a permutation P-box with the same image size by a logistics map, which completely upsets the positions of the pixels. Theoretical analyzes and computer simulations verify the feasibility and the superiority of the proposed encryption algorithm, see the diagram of our proposed system. 6.

This document is organized as follows. In section 2, the confusion function generated by the Henon-Lozi function is introduced. In section 3, the logistic function and the permutation operation based on it are introduced. In section 4, the decryption algorithm, In section 5, performance analyzes and simulation results are reported. Section 6 gives some conclusions.

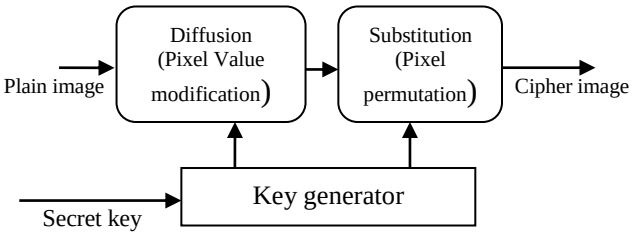


Fig. 1. General architecture diffusion-permutation

II. CONFUSION OPERATOR BASED ON THE HONON-LOZI ATTRACTOR:

A. *The Hénon-Lozi Attractor [6] :*

The attractor defined by the following system of equations (1), where a, b are constants:
The initial values of X_0, Y_0 and a, b are considered the secret key.

$$\begin{cases} X(n+1)=1+Y(n)-a*|X(n)| \\ Y(n+1)= b*X(n) \end{cases} \quad (1)$$

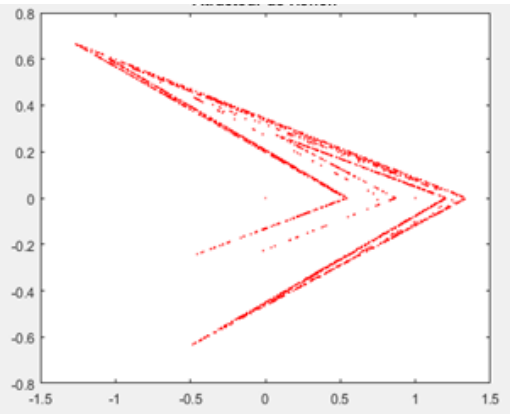


Fig. 2 . The Henon-Lozi Attractor.

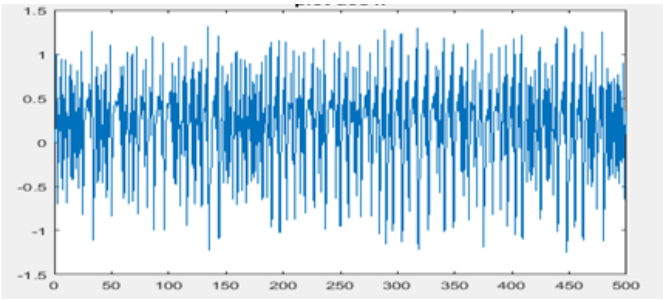


Fig.3 . Plot of X.

B. *Confusion operator based Henon-lozi system:*

- Henon-Lozi map was used to generate a confusion matrix of the same size of the original image. (We use as key the initial parameters of the Henon-Lozi function a, b, X0, Y0).

- We combine with an exclusive or XOR (bit by bit) between the pixels of the image in clear and the matrix of confusion generated by the first function (Henon-Lozi map).

Algorithm that generates the 'mat-conf' confusion matrix:

```
r=row*col ;
x=zeros(1,r);
y=zeros(1,r);
x(1)=x0;
y(1)=y0;
for n=1:r-1
   x(n+1)=1+y(n)-a*abs(x(n));
   y(n+1)=b*x(n);
end
for n=1:r
mat-conf(n)=mod(fix(x(n)*10^7),256)+1;
 end
```

III. PERMUTATION OPERATOR BASED ON LOGISTIC MAP :

A. *Logistic map [7]:*

The logistic map shown in (2) is a discrete chaotic system when the parameter μ between 3.57 and 4. Here, the initial value X_0 and the parameter μ are considered as the secret key.

$$Xn+1 = \mu * X_n * (1-Xn) \qquad (2)$$

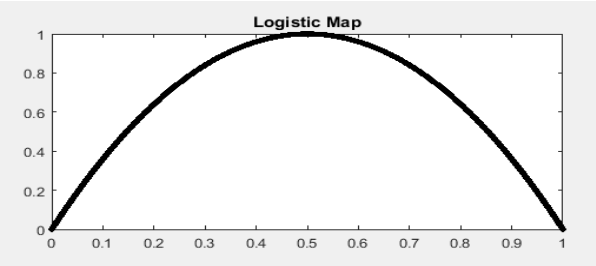


Fig. 4. The Logistic MapEquations.

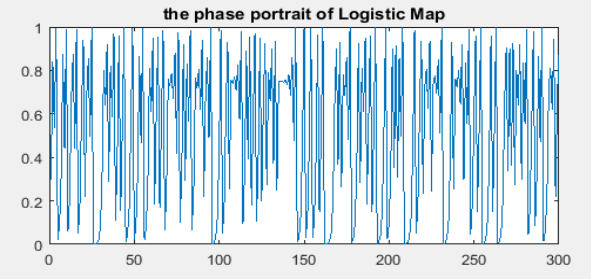


Fig. 5. The phase portrait of Logistic Map

B. *Permutation Operator based on Logistic map:*

For a gray scale image 256 of size M × N, it is an integer matrix of M rows and N columns, in which the values range from 0 to 255. Its data can be treated as a one-dimensional vector
A = {a1, a2, .., a_{MN}} where ai designates the gray level of the image pixel in the column (i/N) column mod (i, N).
Given x_0 and μ, to change the pixel position of the image, we take the following steps:

- **Step 1 :** Iterate the logistic map xi + 1 = F (x) using equation (2) for L times when L> M * N. and obtain P'= {x1, x2, ..., xMN, ...xL}.
- **Step 2** : Obtain an entire random sequence P"according to the following formula: for i = 1: L make p"(i) = mod (fix ((10 ^ 2) * x (i)), MN) +1;
- **Step 3** : uses P = unique (p", 'stable') the function MATLAB returns the same data as in p", but without repetitions and P is in the same order as p".
- **Step 4** : use P as our P-box.

Unlike traditional block-based encryption methods such as DES and AES, the proposed algorithm completely swaps the pixel positions of the image, using a P-box with the same simple image size.

IV. THE ALGORITHM OF DECRYPTION:

The decryption procedure is similar to that of the encryption process in reverse order:

Step1: Generation of P-box by the logistic function with the same initial parameters X0,μ.

Step2: Get P' from C (Cipher image)

Step3: Generation of Confusion matrix by the Henon-Lozi.

Step4:We combine with an XOR (bit by bit) between the pixels of the P' and the matrix of confusion generated by the first function (Henon-Lozi map) we get the plain Image.

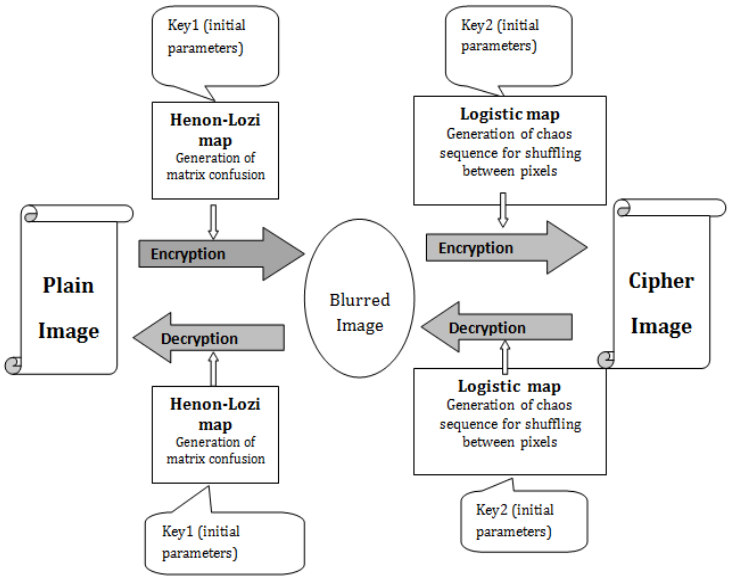


Fig. 6. Diagram of our proposed system

V. PERFORMANCE TEST AND ANALYSIS

A. *Key Space Analysis*

The size of the key space is the total number of different keys that can be used in encryption. A good encryption algorithm should be sensitive to secret keys, and the key space should be big enough to make a brute force attack impossible. In the proposed algorithm, one key one for the logistic function consists of the initial value x0 and the parameter μ, where 3.57 <μ <4. And the second key for the Henon-Lozi attractor consists of the initial values x0, Y0 and a, b; Thus, the proposed algorithm gives a completely different deciphered image for a slightly modified key.

B. *Statistical analyzes*

Shannon suggested that diffusion and confusion should be used in a cryptographic system [8] in order to frustrate powerful statistical analysis. In the proposed encryption algorithm, a sequence of random numbers was generated by Henon-Lozi map to modify the pixel values sequentially which can be considered a confusing process, and after a dynamic P-box generated by a logistics map is used to swap the normal image, which can be considered as a diffusion process.

As a result, the broadcast image is randomly distributed. This is shown by a test on the histograms of the encrypted images in Section C, the correlations between adjacent pixels in the encrypted image and the clear image in Section D, and the information entropy of the encrypted image in section E.

C. *Histograms of the encrypted image:*

Figs. 4 and 5 illustrate the histograms of the "APCsaida" (a) single image and (b) the corresponding encrypted image. The histogram of the encrypted image is almost evenly distributed, which may well protect image information to resist statistical attack [9]

(a)

(b)

Fig. 7. (a) Plain-Image 'APCsaida'- and (b) corresponding Cipher-Image ''

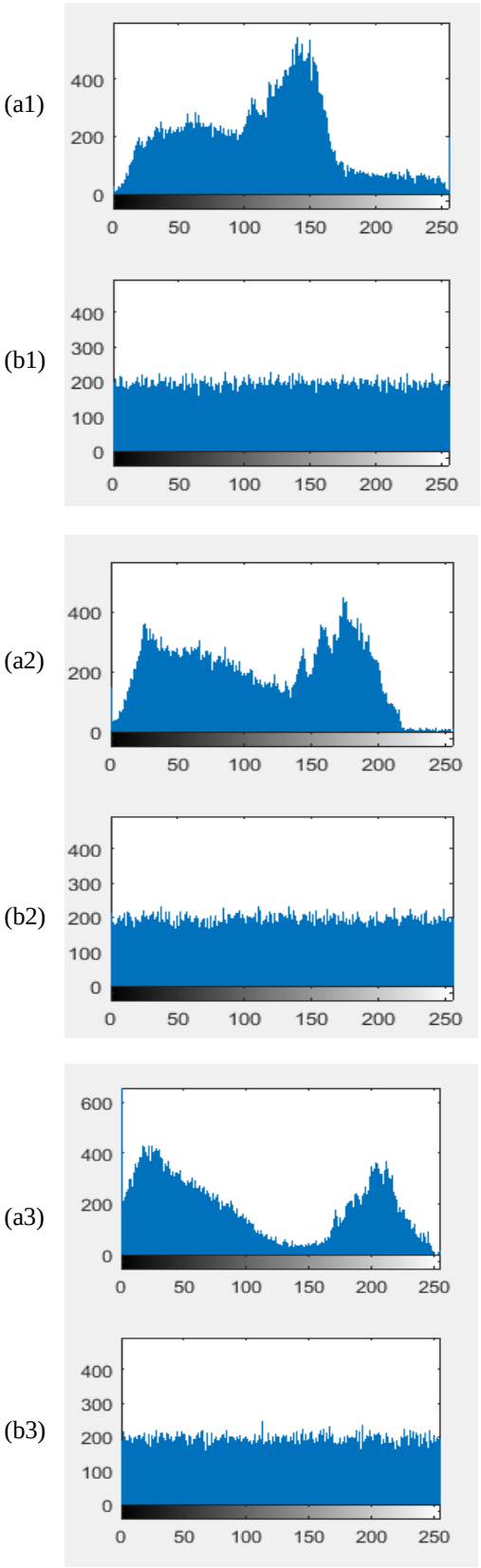


Fig. 8 . Histogram (a) Plain-image 'APCsaida'- (b)Cipher image using proposed method 1:red canal - 2: green canal – 3: blue canal.

D. Correlation of two adjacent pixels:

There is a strong correlation between the pixels of an image that is called intrinsic feature. Thus, a secure encryption scheme should remove it to improve the resistance against statistical analysis. To test the correlation between two adjacent pixels in a single image and an encrypted image, we randomly select a group of adjacent pairs of pixels (vertically, horizontally and diagonally) from the simple image and the encrypted image, and calculate the coefficient of each pair by equation (6).

$$Y_{xy} = \frac{cov(x,y)}{\sigma_x \sigma_y} \quad (3)$$

$$cov(x,y) = \frac{1}{N}\sum_{i=1}^{N}(x_i - \bar{x})(y_i - \bar{y}) \quad (4)$$

$$\sigma_x = \frac{1}{N}\sum_{i=1}^{N}(x_i - \bar{x})^2 \quad (5)$$

$$\sigma_x = \frac{1}{N}\sum_{i=1}^{N}(y_i - \bar{y})^2 \quad (6)$$

Where x and y are gray scale values of two adjacent pixels in the image.

Table 1 shows the correlation coefficients of two pixels adjacent to the image plain and the encrypted image. This correlation analysis proves that the chaotic encryption scheme satisfies zero co-correlation, which is a high-level private security.

TABLE I. CORRELATION COEFFICIENTS OF TWO ADJACENT PIXELS IN THE PLAIN AND THE CIPHER-IMAGE.

Hénon-Lozi map (a=1.7, b=0.5 , x_0=0.2 , b_0=0.2).
Logistic map (μ=4 ; x_0=0.123456).

Direction	Plain-image	Cipher-image by proposed system
Horizontal	0.86696	5.6835 **E**-05
Vertical	0.89084	0.0066414
diagonal	0.80294	-0.0037051

E. Entropy Analysis of Information

Entropy is the most remarkable feature of randomness.
For entropy information H (s) of a message sources can be calculated as (7) [10]:

$$H(s) = \sum_{i=0}^{2^N-1} p(s) \times \log_2\left(\frac{1}{p(s_i)}\right) \quad (7)$$

Where $p(s_i)$ indicates the symbol probability Si. For a true random source emitting 2N symbols, the entropy should be N. Take an image in 256 gray levels for example, and the pixel data have 28 possible values, so the entropy of a "real random» image must to be 8.

The entropy of the encrypted images is shown in Table 2. The values obtained are very close to the theoretical value 8. This means that the leakage of information in the encryption process is negligible and that the encryption scheme is secure when an entropic attack.

TABLE II. ENTROPY VALUE FOR THE ENCRYPTED IMAGE

Canals	Entropy value for plain-image	Entropy value for cipher-image
Canal 1 Red	7.67	7.9971
Canal 2 green	7.6903	7.9964
Canal 3 blue	7.5997	7.9963

F. Sensitivity analysis

In order to test the difference between two images, we measure the NPCR [11] (number of pixels changes rage) and UACI [12] (uniform average changing intensity) by Eqs. (11) and (12).

$$NPCR = \frac{\sum_{i,j} D(i,j)}{w \times H} \times 100 \qquad (7)$$

$$UACI = \frac{1}{w \times H}\left[\sum_{i,j} \frac{|c_1(i,j) - c_2(i,j)|}{255} \times 100\right] \qquad (8)$$

where C1 and C2 are two images of the same size (M × N). If c (i, j) = c2 (i, j) then D (i, j) = 1, else D (i, j) = 0.

TABLE III. NPCR AND UACI VALUES BETWEEN THE ORIGINAL IMAGE AND THE ENCRYPTED IMAGE

Key (Henon-Lozi) a-b-x_0.y_0	Key(Logistic map) x_0.μ	NPCR(%)	UACI(%)
(1.7-0.5-0-0)	(0.123456-4)	99.50	32.51
(1.7-0.5-0-0)	(0.1234560001-4)	99.58	33.56
(1.7-0.5-0-0)	(0.123456-4)	99.61	33.66
(1.7-0.5-0.0001-0)	(0.123456-4)	99.50	32.49

VI. CONCLUSION

In this article, chaos-based image encryption with a diffusion-permutation architecture is proposed. In the broadcast step, the key flow depends on both the key (the initial value and the control parameters of the Henon-Lozi map) and the clear image. In the permutation step, the schema generates a P-box with the same plain-image size by a Logistics map. The key space is large enough to withstand brute force attacks. Statistical analysis shows that the scheme can well protect the image of the statistical attack. The system has a high key sensitivity and has good anti-differential attack capability. With high encryption speed, it can be used in Internet applications.

REFERENCES

[1] S. Li, G. Chen, A. Cheung, B. Bhargava, K.-T. Lo, On the Design of Perceptual PEGvideo Encryption Algorithms, CoRR abs/cs/0501014, 2005.

[2] J. Fridrich, International Journal of Bifurcation and Chaos 8 (1998) 1259.

[3] F. Sun, S. Liu, Z. Li, Chaos, Solitons & Fractals 38 (2008) 631.

[4] Z. Liu, Q. Guo, L. Xu, M.A. Ahmad, S. Liu, Optics Express 18 (2010) 12033.

[5] G. Chen, Y. Mao, C.K. Chui, Chaos, Solitons & Fractals 21 (2004) 749

[6] R. Lozi. UN ATTRACTEUR_ETRANGE (?) DU TYPE ATTRACTEUR DE Henon Journal de Physique Colloques, 1978, 39 (C5), pp.C5-9-C5-10.

[7] May, Robert M. (1976). "Simple mathematical models with very complicated dynamics". Nature. 261 (5560): 459–467.

[8] C.E. Shannon, Bell Systems Technical Journal 28 (1949) 656.

[9] F. Sun, Z.L.S. Liu, Optics Communications 283 (2010) 2066.

[10] A.D. Santis, A.L. Ferrara, B. Masucci, Discrete Applied Mathematics 154 (2006) 2348 Coding and Cryptography.

[11] A.G. Bluman, Elementary Statistics: A Step by Step Approach, WCB/McGraw-Hill,1997.

[12] Y. Mao, G. Chen, S. Lian, International Journal of Bifurcation and Chaos 14 (2004)3613.

Detection and Prevention of Suicidal Self-harm Behavior in Twitter

Hadj Ahmed BOUARARA
GeCoDe laboratory, Dr Molay Tahar university of saida algeria

ABSTRACT

Recently, with the development of communication means such as 4g and the rapid growth of the use of mobile devices (smartphones and tablets) the number of twitter users has increased exponentially. By the end of 2018 twitter has 321 million active users with over 600 million tweets every day. However, all this information will have no use if we cannot access the meaning it carries.

Our idea is to identify twitter users with suicidal or self-harm behaviors by analyzing their tweets using an algorithm inspired from the social life of Asian elephants. The objective is to prevent the situations of depressions, threats of suicide or any other form of self-destructive behavior that exists on Twitter.

Key Words: Self-Harm, Suicidal Behavior, Depressive Person, Asian Elephants, Social Network, Twitter, Datamining, sentiment analysis.

1. INTRODUCTION AND PROBLEMATIC

Twitter strives to provide an environment where users can feel free to express themselves. People's anxiety is reported to have increased 70% since the advent of the internet, according to a study published in 2018 by UK-based Royal Society of Public Health (Araque, 2019). Social networks are a vector of anxiety, sleep problems and depression. Twitter receives in this study, the palm of the worst network for morale.

In 2017, an event prompted them to react: an 18-year-old man posted a tweet explaining his desire to end life on twitter, it was April 24, 2017. The next day, he put an end to his days. A shock for users and a bad buzz for twitter. Since 2017, social networks have been working with suicide prevention associations around the world to provide support to persons in distress (Alaei, 2019).

It is difficult to interpret online publications. Even so, there are some warning signs that can help us to identify people who are suicidal or have a risk of self-harm such as:

Does this person show a sense of depression or hopelessness in his publications?

Does this person publish morbid comments? Does she evoke death unequivocally?

Does this person post comments about past suicide attempts?

Does this person describe or publish photos of self-harm?

In this context our goal is to develop a new system to detect depressive persons with self-harm or self-suicidal behavior using an algorithm inspired from the social life of Asian elephants. This system aims to analyze the feelings of twitter users based on the interpretation of their publications to prevent situations of depression by signaling a self-destructive post.

The general structure of this paper will be as follows: we start with a state of the art for presenting the essential works in this topic, after we go on with a section detailing our approach and proposed components then an experimental and comparative study will be carried out for presenting the best results obtained. Finally, we will finish with a conclusion and describing some lines of thought that remain open and that we want to share them with you.

2. LITERATURE REVIEW (RELATED WORK) :

Our people detection problem with self-harm or suicidal behavior is registered in sentiment analysis field. In what follows we will mention the different works to realize in this context:

The work of Mohammad et al In (Mohammad, 2013) have described two state-of-the-art of SVM classifiers, one to detect the sentiment of messages such as tweets and SMS (message-level task) and one to detect the sentiment of a term within a message (term-level task) followed by the contributions of researcher Nasukawa and his team in 2003 (Nasukawa, 2003) who proposed a new method for extracting associated concepts from segments and summing the orientations of the opinion vocabulary present in the same segment.

In 2018 Mauro Dragoni et al proposed a commonsense ontology for sentiment analysis based on SenticNet, a semantic

network of 100,000 concepts based on conceptual primitives (Dragoni, 2018). In 2006, researchers Kanayama and Nasukawa (Kanayama, 2006) as well as Ding and Liu (Ding, 2008) in 2008 proposed, for their part, a learning-based approach that uses the coordination conjunctions present between a word already classified and a word unclassified.

A new Approach using deep learning was proposed by Cıcero Nogueira dos Santos in 2014 for the analysis of tweets, the authors applied their idea on the corpus STS and they have obtained an accuracy of more than 80% (Dos Santos, 2014). A Multimodal sentiment analysis is a very important growing field of research. A promising area of opportunity in this field is to improve the multimodal fusion mechanism in (Majumder, 2018) Majumder et al have developed a Hierarchical Fusion with Context Modeling based on a Multimodal Sentiment Analysis.

In (Alaei, 2019) different approaches to sentiment analysis applied in the field of data analysis and evaluation of metrics. The paper concludes by outlining future research avenues to further advance sentiment analysis in tourism as part of a broader Big Data approach.

In (Xiang, 2018) a new methodology has been adopted using a machine learning approach with which textual documents are represented by vectors and are used for training a polarity classification model. Several documents' vector representation approaches have been studied, including lexicon-based, word embedding based and hybrid vectorizations. The competence of these feature representations for the sentiment classification task is assessed through experiments on four datasets containing online user reviews in both Greek and English languages, in order to represent high and weak inflection language groups. In (Zheng, 2018) Zheng et al had the idea of sentimental feature selection for sentiment analysis of Chinese online reviews and also in (Proksch, 2019) the authors create a multilingual sentiment-based approach that can effectively capture different types of parliamentary conflict.

In (Araque, 2019) araque et zhu propose a sentiment classification model that uses the semantic similarity measure in combination with embedding representations. In order to assess the effectiveness of this model, the authors perform an extensive evaluation. Experiments show that the proposed method can improve Sentiment Analysis performance over a strong baseline, being this improvement statistically significant.

3. PROPOSED APPROACH :

3.1. THE SOCIAL LIFE OF ASIAN ELEPHANT

Generally, each Asian elephant lives in a group led by a matriarch1 (aged and experienced), who coordinates the movements of the herd. Elephants in each group may be temporarily divided to search for sources of water or food while maintaining contact (pool, 1999).

Elephants communicate with each other directly and discreetly up to 10 km away with an inaudible infrasound for humans (Bates, 2007). The experiments shown that elephants are able to recognize and follow their family members (Bates, 2008). They will join the contact calls sent by his friends from the same group.

The organization of the elephants social life has a practical advantage: when resources are scarce, in the case of drought, for example, links become tighter and elephants in the same group (family) come closer together. Each elephant in a drought situation looks for water points and follows the choice of its congeners. When he finds water points, he sends signals to inform his friends of the place of water. Elephants maintain close ties even after a separation of more than one year (McComb, 2001).

A scenario that summarizes the social phenomenon of Asian elephants in search of food or water points in case of drought is: Initially, a set of elephants are looking for a water point in the space randomly. Elephants do not know where is the water point but they know exactly how far away is and the positions of their elephant friends, then the question that arises: what is the strategy followed to find the water in good conditions? The best solution is to follow the elephants having best position relative to the water point with which have a strong bond of friendship thus to follow the laws of the matriarch who guide the direction of the group.

3.2. PASSAGE FROM NATURAL TO ARTIFICIAL:

This part is dedicated to the passage of the natural life of social Asian elephants to artificial life as shown in the next Table.

[1] The matriarch: she can be a big sister, mother, aunt, grandmother or grand aunt for all the members of her group. She has knowledge of the group; she knows the migratory routes, the rhythm of the seasons and the important places to find water and vegetation.

Table 1: passage from social life to artificial life of social Asian elephants' algorithm

Naturel life of asian social elephants	Algorithm of social Asian elephants
An elephant joins the water point found by his family group	Each user is classified in the most appropriate class (depressive or non-depressive)
Suppose the case where there are only two water points in the search space	Two classes (depressive and no-depressive)
Environnement	Search space (twitter)
Elephant	Twitter user
Group of elephants	The users tweets (corpus)
Matriarch (oldest female)	Represents the message of the person with the highest score in the learning base
Best individual of each elephant group (initialization)	For each class it is the Person who has the best correlation with the centroid (barycenter)
Best individual (in process)	Best fitness function
Friendship link between elephant i and the best individual	α : link between each user and the best individual of each class (depressive or non-depressive)
Friendship link between the elephant I and the matriarch	β : link between each user and the matriarch of each class (depressive or non-depressive)
Communication between the elephant and the best individual	$\left\|ME_{\mathrm{T}}^{g} - E_{\mathrm{T}}^{i}\right\|$
Communication between the elephant i and the matriarch	$\left\|PE_{\mathrm{T}}^{g} - E_{\mathrm{T}}^{i}\right\|$

3.3. THE ARTIFICIAL LIFE OF SOCIAL ASIAN ELEPHANTS' (SAE) ALGORITHM

We have imitated the social life of Asian elephants and their water points search phenomenon in case of drought to formulate a new algorithm to detect depressive behavior by analyzing the users of twitter network. In our problem we have two classes depressive and no-depressive. The user status will be transformed to vectors. Each user with a velocity V is classified according to a fitness function based on his experience, the experiences of other users, the friendship relation that exists with the users of each class and the directives received by the matriarch of each class. The input of the algorithm is a set of twitter users' vectors (corpus), divided into two parts the learning basis and the test basis. The general process is detailed in Figure 1 and the stages of its operation are discussed later:

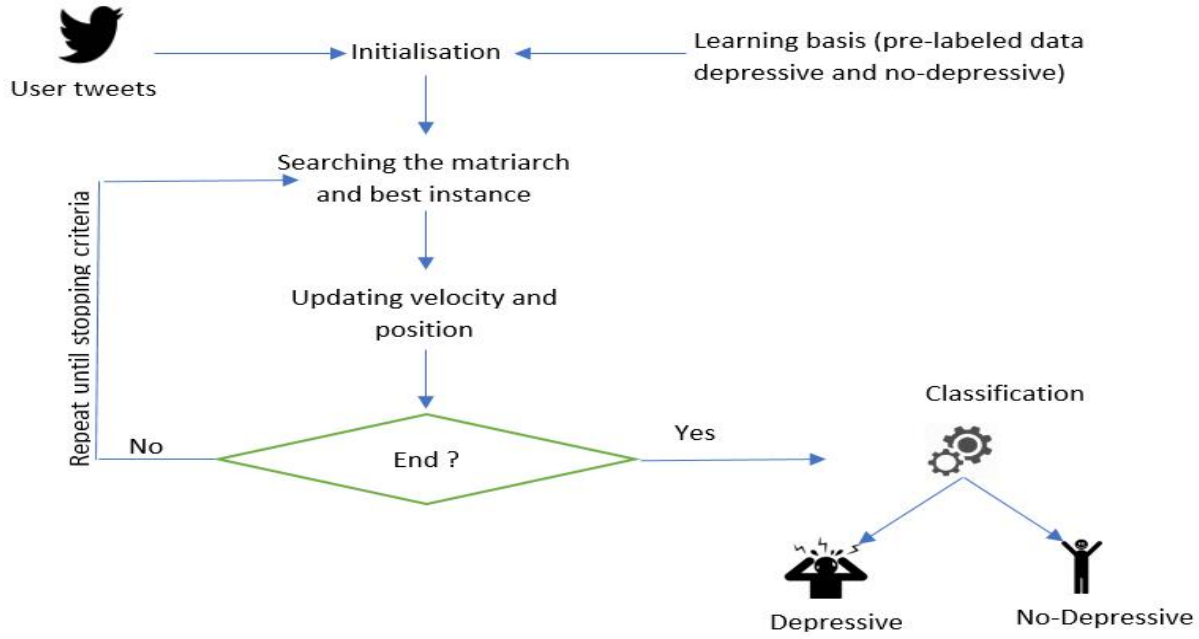


Figure 1 – general architecture of social Asian elephants (SEA) algorithm for depressive person detection.

a. Initialisation

Initially, the position E_0^i and the velocity V_0^i of each user relative to each class g are calculated by the next equations (1) et (2) :

$$\mathrm{V}E_0^i = score(i) \text{ ..... (1)}$$

$$E_0^i(g) = \text{the linear correlation instance i and}$$

the centroid of class g ... ... (2)

- $\mathrm{V}E_0^i(g)$: The initial movement velocity of the user i.
- $E_0^i(g)$: The initial position of the instance t relative to the class g.
- *Score(i)* : The weights sum of the components user vector i.

For the classification of a new instance (of the test database) the following process is launched:

b. Matriarch

We are looking for the matriarch of each class (depressive or no-depressive) that is the user with the highest score (the elephant female, the oldest and the most experienced).

$$Mt(g) = \big(\max\big(score(i)\big)\big)g \quad (3)$$

- $Mt(g)$: The matriarch user at time t in class g.
- $(\max\big(score(i)\big))g$: the user that has the highest score in the class g.

c. Velocity

The movement velocity of each user changes from time t to t + 1 by the equation (4) :

$$VE_{\mathrm{T}+1}^i(g) = \frac{VE_{\mathrm{T}}^i}{\alpha(|ME_{\mathrm{T}}^g - E_{\mathrm{T}}^i|) + \beta(|PE_{\mathrm{T}}^g - E_{\mathrm{T}}^i|)} \quad (4)$$

- VE_{T}^i : The movement velocity of the user i at time t relative to the class g.
- ME_{T}^g : The position of the best user at time t in class g (initially it is the closest user to the centroid of the class).
- E_{T}^i : The position of user i at time t relative to the class g.
- PE_{T}^g : The position of the matriarch of the class g at the time t.
- α : the friendship relation between the best user and the user i.
- β : the friendship relation between the matriarch and the user i.

d. The position (fitness function)

This step calculates the new position of each user relative to each class through the equation (5):

$$E_{t+1}^i(g) = E_t^i(g) + VE_{t+1}^i(\mathrm{g}) \quad (5)$$

- $E_t^i(\mathrm{g})$: position or fitness function of user i at time T in class g.

- g: has two values depressive or no-depressive.
- VE_{t+1}^{i}(g): velocity of user i at time T + 1 in class g

e. Evaluation (classification) and update :

Each user is classified in the class (depressive or no-depressive) with the lowest fitness function. After each iteration the parameters of the algorithm are updated. The same process will be repeated until stopping criterion (number of iteration).

f. Procedure :

The next pseudo code summarizes the functioning of the social elephant algorithm for the detection of depressive people in twitter network.

Social elephants algorithm.

1: Elephant : twitter user

2: input :

3: - corpus (learning basis, test basis)

4: - Initialisation $(\boldsymbol{E_{T=0}^{i}}, \boldsymbol{V_{T=0}^{i}})$

5: $\boldsymbol{T \leftarrow 0}$

7: while not CD do

8: for each tweets user to be classified do

9: for each class g do

10: calculate

11: $\boldsymbol{Mt(g) = (\max(score(i)))g}$

12: find best user ME : with smaller position E

13: $\boldsymbol{VE_{T+1}^{i}(g) = \frac{VE_{T}^{i}}{\alpha(|ME_{T}^{g} - E_{T}^{i}|) + \beta(|PE_{T}^{g} - E_{T}^{i}|)}}$

14: $\boldsymbol{E_{t+1}^{i}(g) = E_{t}^{i}(g) + VE_{t+1}^{i}}$(g)

15: end for

16: $\boldsymbol{L'instance(i) \leftarrow the\ class\ with\ the\ smallest\ fitness\ function}$

17: end for

18: update (ME, M, V)

19: $\boldsymbol{T \leftarrow T + 1}$

20: end while

21: output : the class of each user from the test basis.

For the vectorization of user tweets we use: i) text cleaning by eliminating special characters and numbers. ii) transforming tweets to a set of terms using bag of words, stemming or n-gram characters. ii) coding using TF (Term Frequency) or TF * IDF (term frequency * inversed document frequency).

4. **Tweets2011 corpus (tweets):**

In our experiments we used the Tweets2011 corpus that was used in information retrieval famous competition called TREC 201. This specialized body built to keywords. The authors of this corpus have used the API to retrieve Twitter4J 649 tweets where they used keywords (politics, cinema, sport, music, war, science). After TREC in 2012 these tweets were classified in two class (depressive tweet, tweet not depressed) (McCreadie, 2012). The following table summarizes the classification of tweets.

Table 2: General Statistical Dataset Tweets2011.

Category	Depressive	not depressive
Cinema	85	62
Policy	49	33
War	64	13
Sport	33	58
Music	119	56
Science	19	58

5. Validation measures :

To validate our results, we have used different metrics that exist in literature such as recall, precision, f-measure, kapa static true positive, false positive, false negative and true negative (Oksuz, 2018).

6. Results and discussion:

In order to validate the quality of our proposal we have applied an experimental protocol by varying:

- Text representation methods.
- We set the parameters Alpha = 1 and beta = 1.
- Number of iteration.

with objective is to identify the sensitive parameters, we have fixed in each test one parameters and varying the others. We calculate the f-measure, entropy, recall precision kappa static. The best results are illustrated in the following tables.

NB : The boxes colored in blue represent the best results and the boxes colored in red represent the bad results.

a. Result with variation of text representation:

As a result of the different languages that exist in the world, finding the best message representation technique is a very important task. In this part, we set each time the technique of representation of text (N-grams-characters with N of 2 to 5 and bag of words) and we vary the other parameters. The results are shown in the next table and figures.

Table 3: the results of analysis using the Asian elephant's algorithm for detecting depressive person in twitter with variation of representation techniques.

		Evaluation measures							
		Precision	**Recall**	**f-measure**	**TS (%)**	**TE(%)**	**static kappa**	**Confusion matrix**	
Text representation techniques	**Bag of words**	0. 724	0. 699	0.7	67.79%	32.21%	0354	258	98
								111	182
	Stemming	0. 786	0617	0.6913	68.72%	31.28%	0386	228	62
								141	218
	2-gram characters	0.819	0.7235	0.769	75.19%	24.81%	0.5038	267	59
								102	221
	3-gram characters	0.86	0.764	0811	79.81	20.19	0.596	282	44
								87	236
	4-gram characters	0.918	0.791	0.854	84.12%	15.86%	0688	292	26
								77	254
	5-gram characters	0844	0.764	0802	78.58	21.42	0.56	282	52
								87	228

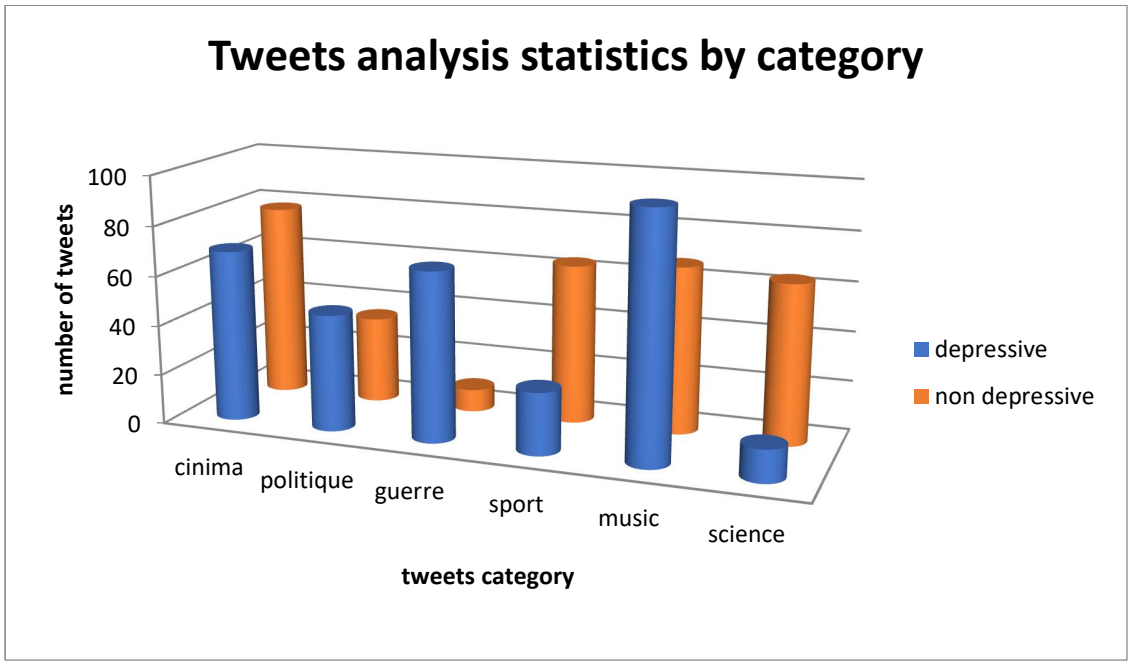


Figure 2: Number of tweets depressive and not-depressive obtained by the Asian elephants algorithm classified by categories

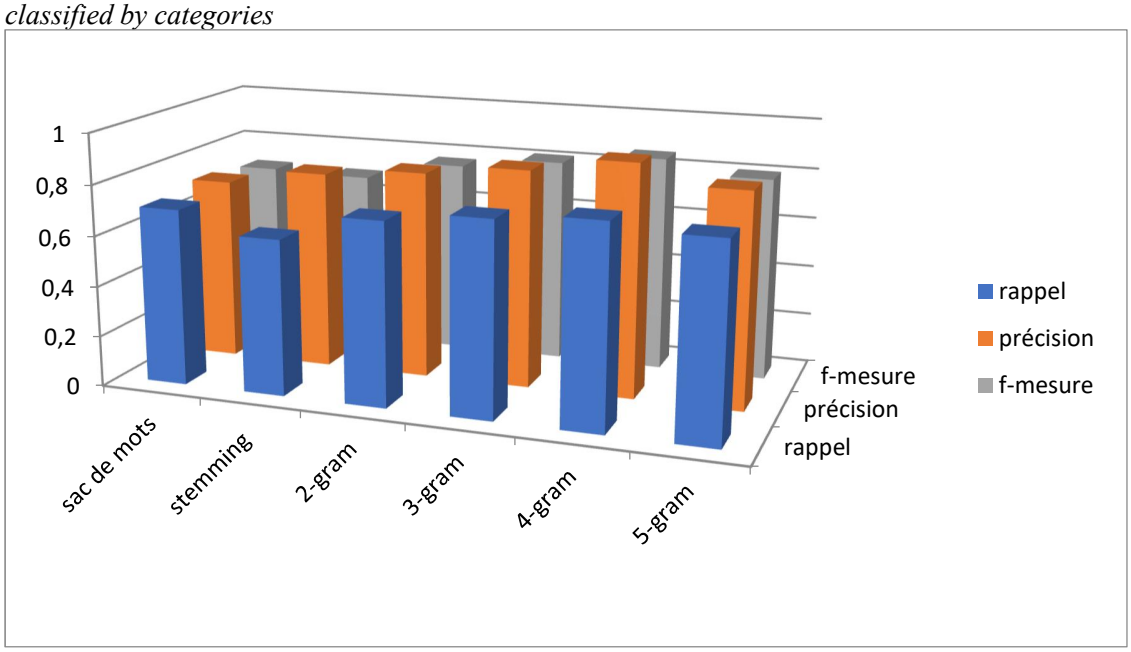


Figure 3: Comparison of text representation techniques results using the Asian elephants algorithm

By observing the table 3 and the previous figures (2 and 3) we found that the technique N-grams characters (the blue boxes) allows to obtain the best results compared to the representation bag of words with a F = 0.85, TS = 84% and kappa static = 0.68. A discussion

and interpretation of the different results is detailed below:

- The n-gram representation is tolerant to the problems of copy-and-paste technology and especially when copying a tweet from a PDF document, a Word document or from a web page.
- Some characters of the copied words will be imperfect for example, it is possible that the word "text-mining" is copying "text-ining". A word bag method will have trouble recognizing that it is the word "mining" whereas the technique N-grams characters takes into account other N-grams like 'ini', nin and i
- ng to recognize the word . It can also detect compound words such as "united state" or "data mining", but the word bag method ignores them.
- The bag of word technique requires a semantic and syntactic treatment to remove the ambiguity related to the words and sentences, which is not the case in our work where we have not applied linguistic treatment on the texts because the computer implementation of these procedures is relatively cumbersome. On the other hand, the N-grams technique is independent to the language and makes it possible to treat the tweets of the users in their raw states
- the major drawback of the stemming technique is the loss of complete information on the terms since it is not based on powerful linguistic constraints, which can lead to an amplification of noise and semantic confusions by grouping under the same root words of different meanings. Like the lexical root "port" which groups in the same set the verb "to wear" and the name "port" whereas semantically are very distinct. On the other hand, the technique n-grams is perfectly adapted for texts coming from noisy source and it can lead us to obtain free the roots of the words. For example, the words advance, advance, advance, and advancement automatically have much in common when considered as sets of N-grams. Another advantage is its ability to work with both short and long documents.
- The representation N-grams is dependent on a parameter N and the question which arises: What is the value of N optimal? Analyzing the returned results, we find that N = 4 has spawned the production of relevant terms to allow the Asian elephants algorithm to differentiate between depressive tweets and not-depressive tweets.

b. Results with variation of iteration number:

Table 4 and Figures (4 and 5) summarize the influence of the parameter iteration number in the obtained results.

Table 4: the analysis results using the Asian elephants' algorithm and variation of distance measures.

		Validation Measures							
		Precision	**Recall**	**f-measure**	**TS (%)**	**TE(%)**	**static kappa**	**Confusion matrix**	
Distances measures	**10**	0.74	0.59	0.654	65.48%	34.52%	0313	221	76
								148	204
	40	0.918	0.791	0.854	84.12%	15.86%	0688	292	26
								77	254
	80	0.781	0715	0.745	72.41%	27.59%	0.45	264	74
								105	206
	120	0.7217	0674	0.699	66.71	33.29	0347	249	96
								120	184

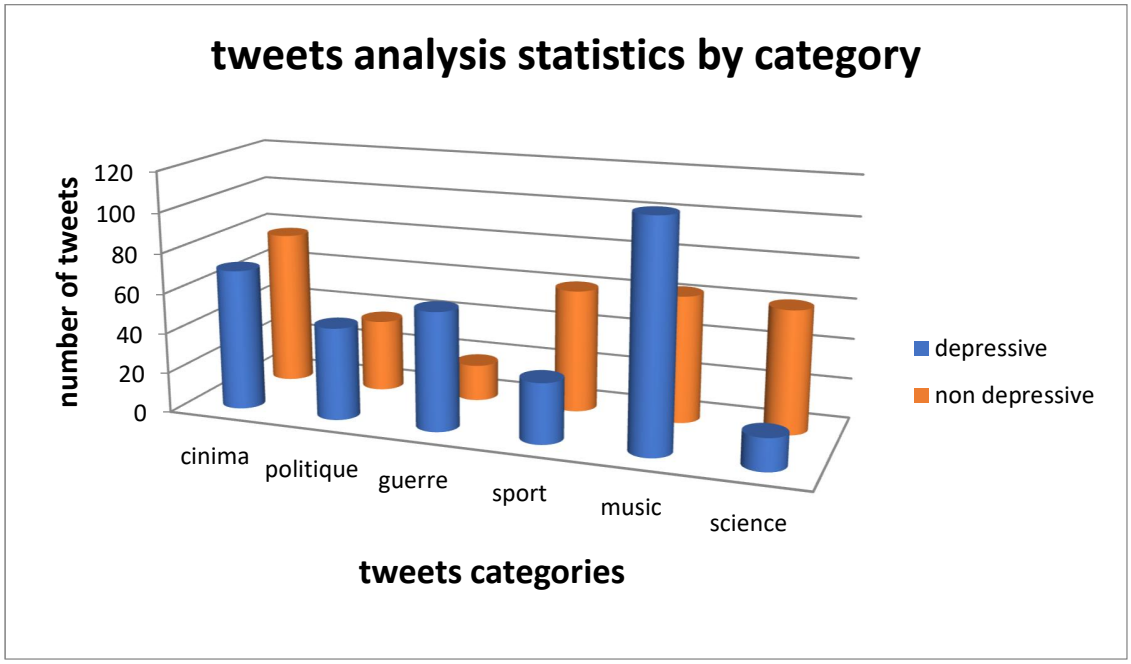


Figure 4: the results of analysis using the asian elephants algorithm for detecting depressive person in twitter with variation of iterations number.

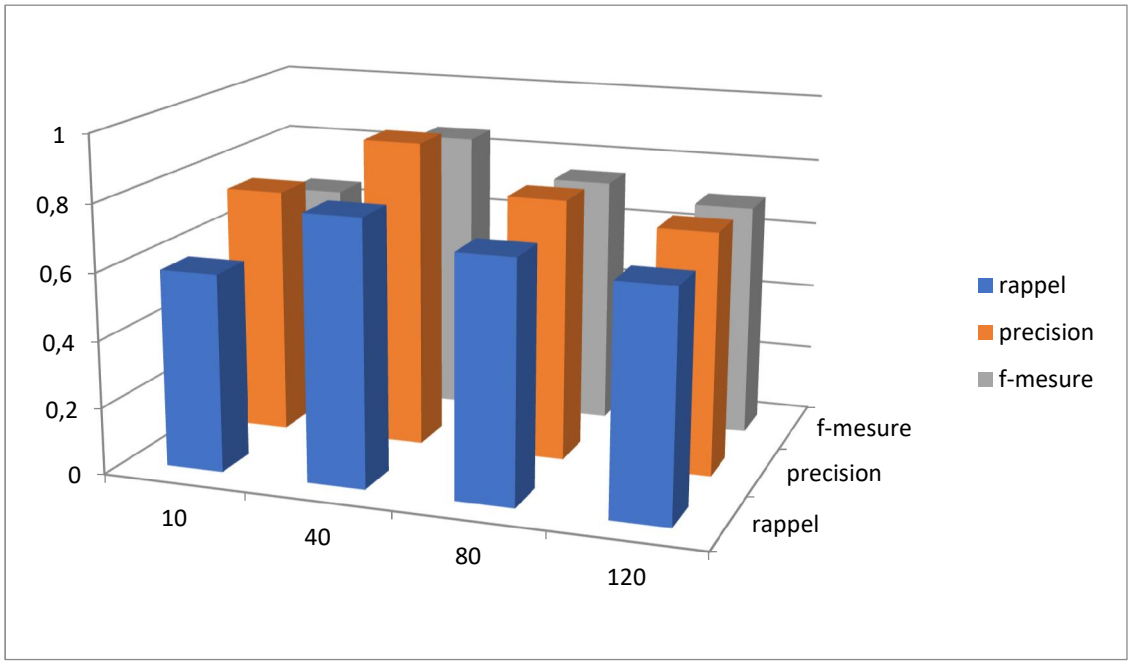


Figure 5: comparison of distance measurements using Asian elephants.

The results clearly show that the stopping criterion is a sensitive parameter because the quality of results of the social elephant algorithm change with the variation of the iterations number.

Comparative study :

in order to reference the results of our algorithm we conducted a comparative study with classical techniques (naive bayes, decision tree, KNearest Neighbor) and with bioinspired techniques integrated in the EBIRI tool (machine heart lungs and social cockroaches algorithm (Bouarara, 2017).

Table 5: comparison results of the social elephant algorithm with other algorithms that exist in the literature for the problem of depressive person detection.

		Valuation Measures							
		Precision	Recall	f-measure	TS (%)	Recall(%)	static kappa	Contingency Matrix	
Algorithms	Naive bayes	0.781	0715	0745	72.41%	27.59%	0.45	264	74
								105	206
	Decision tree	0608	0.51	0558	53.62%	46.48%	0.09	190	122
								179	158
	Asian elephants algorithm	0918	0791	0854	84.12%	15.86%	0688	292	26
								77	254
	Social cockroaches Algorithm	**0.92**	**0.74**	**0.82**	**82.43**	**17.57**	**0.65**	**276**	**21**
								93	**259**
	Heart lung machine	**0.88**	**0.82**	**0848**	**84.28**	**15.72**	**0.68**	**306**	**39**
								63	**241**

The results of this part validate our originally set goal where our algorithm is better than the like algorithms and gives the same performance as the algorithm because our proposal is based on the principle that the solution needs to improve from iteration to another through the intelligence of the group.

7. CONCLUSION

detecting depressed people is a very difficult task because the feelings of people are not stable and can change from one minute to another and especially based on information shared in virtual world (tweeter). According to our results we notice that Asian elephant's algorithm gives better performances compared to others classical and bioinspired algorithms.

Finally, we propose that Social network owners must add an option to analyze the status of each user to say that a person is in a normal or depressive situation by suggesting those users to:

- Consult a doctor or psychologist because There are many effective treatment modalities against depression, including medications (eg antidepressants) and psychotherapy.
- Get as much information as possible about depression and how it is treated. This will allow you to understand what is happening to you and make informed decisions.
- Adopt a healthy lifestyle and Work less if necessary, avoid sources of unnecessary stress, allow yourself hours of rest and sleep, and eat well are all measures that can help you get back on your feet quickly.

7.1. FUTURE WORKS

We will apply the algorithm to the problem of suspicious person detection, spam filtering, DNA

classification, information retrieval, sentiment analysis in video, plagiarism detection, and all classification problem supervised or unsupervised.

References:

McCreadie, R., Soboroff, I., Lin, J. Macdonald, C., Ounis, I., & McCullough, D. (2012, August). One building has reusable Twitter corpus. In Proceedings of the 35th International ACM SIGIR conference on Research and development in information retrieval (pp. 1113-1114). ACM.

Bouarara, HA, & Hamou, RM (2017). Bio-Inspired Environment for Information Retrieval (Ebiri): innovations from nature. European academic editions.

Mohammad, S. M., Kiritchenko, S., & Zhu, X. (2013). NRC-Canada: Building the state-of-the-art in sentiment analysis of tweets. arXiv preprint arXiv:1308.6242.

Nasukawa, T., & Yi, J. (2003, October). Sentiment analysis: Capturing favorability using natural language processing. In Proceedings of the 2nd international conference on Knowledge capture (pp. 70-77). ACM.

Dragoni, M., Poria, S., & Cambria, E. (2018). OntoSenticNet: A commonsense ontology for sentiment analysis. IEEE Intelligent Systems, 33(3), 77-85.

Kanayama, H., & Nasukawa, T. (2006, July). Fully automatic lexicon expansion for domain-oriented sentiment analysis. In Proceedings of the 2006 conference on empirical methods in natural language processing (pp. 355-363). Association for Computational Linguistics.

Ding, Y., Liu, X., Zheng, Z. R., & Gu, P. F. (2008). Freeform LED lens for uniform illumination. Optics Express, 16(17), 12958-12966.

Dos Santos, C., & Gatti, M. (2014). Deep convolutional neural networks for sentiment analysis of short texts. In Proceedings of COLING 2014, the 25th International Conference on Computational Linguistics: Technical Papers (pp. 69-78).

Majumder, N., Hazarika, D., Gelbukh, A., Cambria, E., & Poria, S. (2018). Multimodal sentiment analysis using hierarchical fusion with context modeling. Knowledge-Based Systems, 161, 124-133.

Xiang, R., Long, Y., Lu, Q., Xiong, D., & Chen, I. H. (2018, October). Leveraging Writing Systems Change for Deep Learning Based Chinese Emotion Analysis. In Proceedings of the 9th Workshop on Computational Approaches to Subjectivity, Sentiment and Social Media Analysis (pp. 91-96).

Zheng, L., Wang, H., & Gao, S. (2018). Sentimental feature selection for sentiment analysis of Chinese online reviews. International journal of machine learning and cybernetics, 9(1), 75-84.

Proksch, S. O., Lowe, W., Wäckerle, J., & Soroka, S. (2019). Multilingual sentiment analysis: A new approach to measuring conflict in legislative speeches. Legislative Studies Quarterly, 44(1), 97-131.

Alaei, A. R., Becken, S., & Stantic, B. (2019). Sentiment analysis in tourism: capitalizing on big data. Journal of Travel Research, 58(2), 175-191.

Poole, J. (1999). Signals and assessment in African elephants: evidence from playback experiments. Animal Behaviour, 58, 185-193

McComb, K., Moss, C., Durant, S. M., Baker, L., & Sayialel, S. (2001). Matriarchs as repositories of social knowledge in African elephants. Science, 292(5516), 491-494.

Finegold, J. A., Asaria, P., & Francis, D. P. (2013). Mortality from ischaemic heart disease by country, region, and age: statistics from World Health Organisation and United Nations. International journal of cardiology, 168(2), 934-945.

Bouarara, H. A., Hamou, R. M., & Amine, A. (2015). New Swarm Intelligence Technique of Artificial Social Cockroaches for Suspicious Person Detection Using N-Gram Pixel with Visual Result Mining. International Journal of Strategic Decision Sciences (IJSDS), 6(3), 65-91.

Araque, O., Zhu, G., & Iglesias, C. A. (2019). A semantic similarity-based perspective of affect lexicons for sentiment analysis. Knowledge-Based Systems, 165, 346-359.

Oksuz, K., Can Cam, B., Akbas, E., & Kalkan, S. (2018). Localization recall precision (lrp): A new performance metric for object detection. In Proceedings of the European Conference on Computer Vision (ECCV) (pp. 504-519).

PSO Variants for Localization Challenge in Wireless Sensor Network and Internet Of Thing

BAIDAR Lotfi
LabRI-SBA Lab.,
Ecole Superieure en Informatique
Sidi Bel Abbes, Algeria
l.baidar@esi-sba.dz

RAHMOUN Abdellatif
LabRI-SBA Lab.,
Ecole Superieure en Informatique
Sidi Bel Abbes, Algeria
a.rahmoun@esi-sba.dz

LORENZ Pascal
IUT of Colmar,
University of Haute Alsace
Mulhouse ,France
Lorenz@ieee.org

MIHOUBI Miloud
EEDIS Laboratory ,
Djillali Liabes University
Sidi Bel Abbes , Algeria
miloud.mihoubi@univ-sba.dz

***Abstract* — Wireless Sensor Network (WSN) has recently been extensively investigated due to their numerous applications where processes have to be spread over a large area. One of several technical aspects of WSNs is the node localization. Most approaches in the recent literature rely on algorithms that maximize the localization rate with a minimum runtime. In this paper, we introduce a comparative study about the PSO (particle swarm optimization) and its variants, The node localization problem is seen as an optimization problem in a multi-dimensional space, PSO computes iteratively (through evolution) the nodes positions using the Euclidian distance as fitness. Deploying this algorithm on a large WSN with hundreds of sensors shows pretty good performance in terms of node localization, two network topology are treated in this paper for contributing the advantages of range communication as an influencing factor.**

Keywords— Particle Swarm Optimisation Wireless sensor network, Optimisation problem , node localization.

I. INTRODUCTION

WSN (Wireless Sensor Network) consists of a large number of densely deployed nodes which are tiny, low power, inexpensive, multi-functional connected by a wireless medium. Its main task is to provide information of environment at each moment, the sensors are installed for tracking and monitoring the environmental requirements and physical phenomenon such as climate prediction, analysis of sane, atmospheric pressure, etc. WSN is employed are several application domains such as security and surveillance, data aggregation, environment sensing, industrial process control, structural health monitoring [1].

The gathered information needs to be associated with sensor nodes rental to provide an accurate view of the sensor field.

Each sensor can monitor its region and proceed to send the collected data to sink node, the effectiveness of WSN is bound to its ability to collect data and transmit them in a minimum time and with greater precision [2].Numerous challenges are addressed in WSN and have been largely browsed: energy minimization (optimization), energy harvesting, compression schemes, self-organizing network algorithms, routing protocols, security, quality of service management, etc…

The three most essential problems are energy efficiency, quality of service and security management [3], moreover, one of the most issues in WSN is node localization, the information location plays a vital role in coverage, deployment purpose, routing information, location service, target tracking, and rescue operations.

The intuitive solution is to equip every node with a Global Positioning System (GPS) receiver that can accurately provide the sensors with their exact location, localization by equipping each node with GPS is not suitable, because it is less energy efficient and expensive, it needs large size of hardware and has a line of sight problem. On the other hand, If GPS is installed on every node, then it increases the node size and deployment cost. Furthermore, GPS is not energy efficient as it consumes a lot of energy and not suitable for a network like WSN, where for instance, it does not work at all in indoor environments.

Numerous localization methods have been proposed for solving the problem, in place of equipping each node by a GPS, the majority of methods allowed to use a certain number of nodes in the network equipped with GPS. These nodes are generally known by anchor nodes, beacons or landmark which their position is known, the remain sensors communicate with the anchor nodes for determinate its positions by using some localization algorithm.

This paper is divided into eight sections, section two gives an overview treatment of node localization problem by metaheuristic algorithm where related work is presented and analysed in this section, the node localization problem is formulated in section three, In the fourth section a comparative study is presented and analysed to evaluate the performance of the proposed algorithm, Our conclusion is drawn in the final section.

II. RELATED WORK

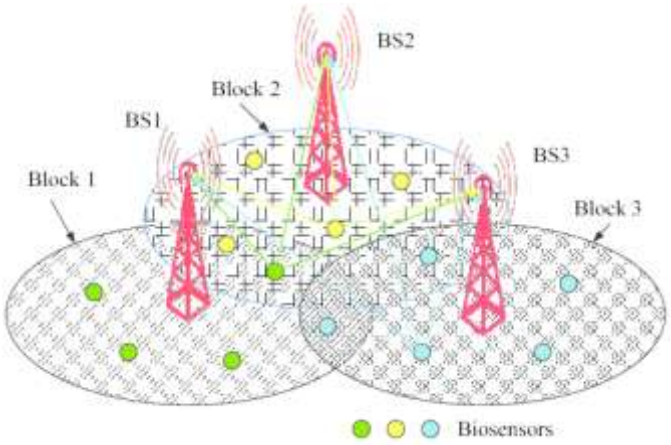


Fig. 1:Localization scheme

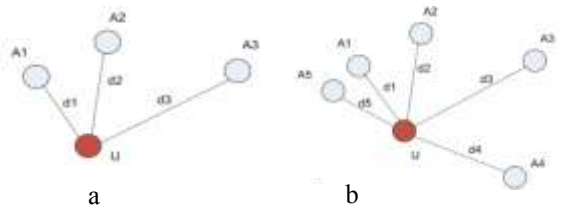
Several surveys on localization are detailed in [4-8] and node localization can be divided via much consideration and according to several criteria: the mobility of the nodes (static vs. mobile, mixed), the execution environment (centralized vs. distributed, mixed), distance estimation (range-free and range-based).

Localization scheme can be divided into three components combined show Fig. 1, where several methods are proposed the first phase (distance estimation).

The main task of the first phase is evaluating the distance between beacons nodes and target nodes, where many techniques are used , we found Radio Signal Strength Indicator (RSSI) [9], Time of Arrival (TOA) and Time Difference of Arrival (TDOA) [10], Angle of Arrival (AOA)[11] are applied to calculate the angle or distance [12].

The selection of distance estimation in localization scheme is an important factor that influences the final performance of the system and that each one is specified according to the field of application.

The second phase named position computation, by exploiting the data from distance estimation phase, it is possible to calculate the coordinates of the target nodes, wherein the several approaches are proposed in this phase: such methods include trilateration (Fig. 2.a), multi-lateration(Fig. 2.a), triangulation, probabilistic approaches, bounding box, the central position, fingerprinting [13], there is other work concentrates all information about distances computing that uses mathematical optimization techniques to compute the positions of the nodes.



a b

Fig. 2: (a) trilateration, (b) Multilateration

The third phase of localization scheme is localization algorithm, the combining operation schematized in Fig. 1, localization algorithm determines how the information concerning distances and positions is manipulated in order to allow nodes of a WSN to estimate their positions.

Localization algorithm has received much attention in the last two years, recently, metaheuristic methods have been seen as important tools to solve the problem of optimization, and node localization is treated as a multidimensional optimization problem, where a substantial number of methods are addressed through population-based stochastic techniques.

PSO (particle swarm optimization) is proposed [14] for node localization problem. After getting the estimated distances and calculated coordinates in the network by the estimation and calculation phases.

The basic idea of this approach that all unknown nodes send the coordinates and distance to a base station, the base station runs PSO to minimize the tracking error defined. The approach does not take into account the flip ambiguity problems (Fig. 3), and location of nodes that do not have at least three tags in their neighborhood, The system only works well if either beacon have sufficient range or there is a large number of beacons. In addition, the base station requires estimates the range of all target nodes located in the surrounding of beacons nodes. This requires a lot of communication that can lead to congestion, delays and the depletion of energy. More than, the proposed scheme has limited scalability because the dimensionality PSO is twice the number of target nodes.

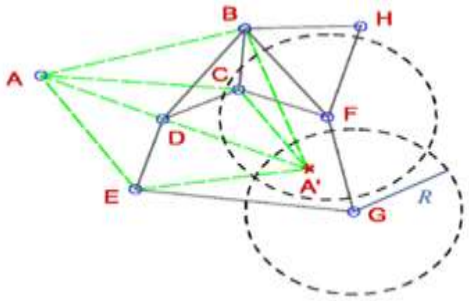


Fig.3:Flip ambiguity phenomenon

PSO approach BFA are proposed [15] to deal with the localization issue, the distributed architecture is utilized for both approaches, iterative fashion to locate the nodes, this means that each target node that has three or more beacons in its hearing range runs localization Algorithm to minimize the localization error, and each node localized in the iteration i is considered as an anchor nodes at iteration i+1 .

The process continues iteratively until either all the nodes get localized or no more nodes can be localized, the proposed method does not require that each node transmit it range measurement to a central node. Besides, it can localize all nodes that have three beacons nodes in their range. As the localization iterations pass by, a node may get the number of references for localization, which mitigates the

flip ambiguity problem, the situation that results in large localization error when the references are near collinear. However, the proposed method is prone to error accumulation.

A comparison of the performance of PSO and BFA in the number of nodes localized, localization accuracy and computation time is presented according to the results, it has concluded that the two approaches have a trade problem where simulations obtained showed that PSO is convergent quickly by contribution to BFA, on other hand BFA gives many error accuracies than PSO .

Binary PSO is proposed to minimize localization time and energy computing and Improving the original approach, where the same strategy of localization phase utilized in [16], this approach has proven effective in comparison with the original approach, although it is efficient in terms of convergent but localization error remains low than the original PSO.

h-best PSO is proposed for enhancement of PSO for node localization problem [17], the objective of the proposed approach is to have a fast converging for localization and have a significant localization rate in terms of nodes and minimizing the location error, the results obtained demonstrated that the proposed approach is efficient when compared with PSO original and BBO, Although The HPSO-based localization algorithm determined the accurate coordinates Quickly, whereas BBO-based localization algorithm find the coordinate of the nodes more accurately. The proposed algorithms also reduce the number of transmissions to the base station, that helps the node to retain more energy, and so, the node can perform for a long period.

in [18], a comparative study is presented in this paper, and three famous metaheuristics: PSO, SFLA, FFA are proposed for node localization in distributed scheme range based, several parameters are combined in comparison as execution time, localization error, number of the non-localized node. For understanding the performance of the proposed algorithms, LabVIEW platform is used. The obtained results show that the PSO converge rapidly then FFA and SFLA algorithms but it gives more average error then the two other. The point common is that there is not the grand difference in the errors offered by both, the selection of the algorithms to use for localization depends entirely on the hardware available to the user and the time constraints involved. The using of short transmission radius is not suitable for these algorithms.

III. NODE LOCALIZATION PROBLEM FORMULATION AS OPTIMIZATION PROBLEM

The main objective of localization is to find out the coordinate of target nodes by using anchor nodes with single hop range-based distributed technique.

The main steps of node localization scheme are:

1/ M target nodes and N anchor nodes are randomly deployed in the sensor field. Each target node and anchor node has transmission range R. Anchor nodes compute their location awareness and transmit their coordinates. The nodes which get settled at the end of iteration serve as reference nodes during the next iteration and behave like anchors.

2/ the node that falls within transmission range of three or more anchors is considered as localized node.

3/ each localized node measures its distance from each of its neighbouring anchors. The distance measurements are corrupted with Gaussian noise n_i, due to environment consideration. A node estimates its distance from ith anchor as $\widehat{\boldsymbol{di}} = [d_i + n_i]$,where d is actual distance given by:

$$\boldsymbol{d_i} = \sqrt{(\boldsymbol{x} - \boldsymbol{x_i})^2 + (\boldsymbol{y} - \boldsymbol{y_i})^2} \quad \text{.....(1)}$$

Whereas (x, y) is the location of the target node and $(\boldsymbol{x_i}, \boldsymbol{y_i})$ is the location of the ith anchor node in the neighborhood .

4/ each localizable node runs meta-heuristic algorithmindependently to localize itself by finding its coordinates (x, y). The objective function (mean of square of error between actual and estimated distances of computed node coordinates and the actual node coordinates), is minimized by:

$$\boldsymbol{f(x,y)} = \frac{\boldsymbol{1}}{\boldsymbol{N}} \sum_{\boldsymbol{i=1}}^{\boldsymbol{N}} \sqrt{(\boldsymbol{x} - \boldsymbol{x_i})^2 + (\boldsymbol{y} - \boldsymbol{y_i})^2} - \widehat{\boldsymbol{di}} \quad (2)$$

Where N ≥ 3 (2D location of a node needs minimum 3 anchors) is the number of anchors with in transmission range, R, of the target node..

5/ evolves the optimal location of target nodes, i.e. (x, y) by minimizing the error function

6/ after coordinates of all localizable nodes (say, ML) are determined, the mean localization error is computed as the mean of square of distance so of computed nodes coordinates $(\boldsymbol{x_i}, \boldsymbol{y_i})$ and the actual node coordinates (X_i , Y_i) ,for i = 1, 2, ML determined for metaheuristic algorithm, as shown below:

$$\boldsymbol{E_L} = \frac{\boldsymbol{1}}{\boldsymbol{M}} \sum_{\boldsymbol{i=1}}^{\boldsymbol{L}} \sqrt{(\boldsymbol{x} - \boldsymbol{X_i})^2 + (\boldsymbol{y} - \boldsymbol{Y_i})^2} \quad \text{.....(3)}$$

Where "L=M-N "

7/ Steps 2 to 6 are repeated by number of iteration defined or until all target nodes get localized or no more nodes can be localized. The performance of the localization algorithm is based on EL and MML, where MML = [M - ML] is the number of nodes that could not be localized. Lesser the value of ML and L, better the performance is.

As the iterations progress, the number of localized nodes increases. This increases the number of references available for already localized nodes. A node that localizes using just three references in an iteration k may have more references in iteration k +1. This decreases the probability of the flip ambiguity.

IV. PSEUDO CODE OF LOCALIZATION SCHEME

1- Define topology of WSN
2- Set the perimeter of networks (length and width).
3- Set number of Anchor nodes N
4- Set number of sensor nodes M. , jϵ(1……M)
5- Set the communication range.
6- Calculate real distance between the beacon and each deployed sensor nodes
7- Call RSSI to estimate the distance between the beacon nodes and each sensor nodes. (1)
8- Call Trilateration or Multilateration to determinate the coordinates of sensor nodes. (2)
9- While (K <M) OR I < nbr_iteration Do
For j=1: M Do
Initialize K (settled nodes) .
Call (Algorithm localization):
(i) Input: (initialize the parameters)
(ii) Call the objective function (2) .
(iii) Output: 1- returns the coordinates (x , y) such that error is minimized.
: 2- plot the coordinates on the figure
K=K+1;
End.
N=N-1;
10- Calculate the localization error (3).
11- end
12- Performance evaluation of the localization algorithm via several criteria:
(i) The localization error versus step size, versus scale factor …etc.
(ii) Number of node localized.
(iii) Display the results.
End.

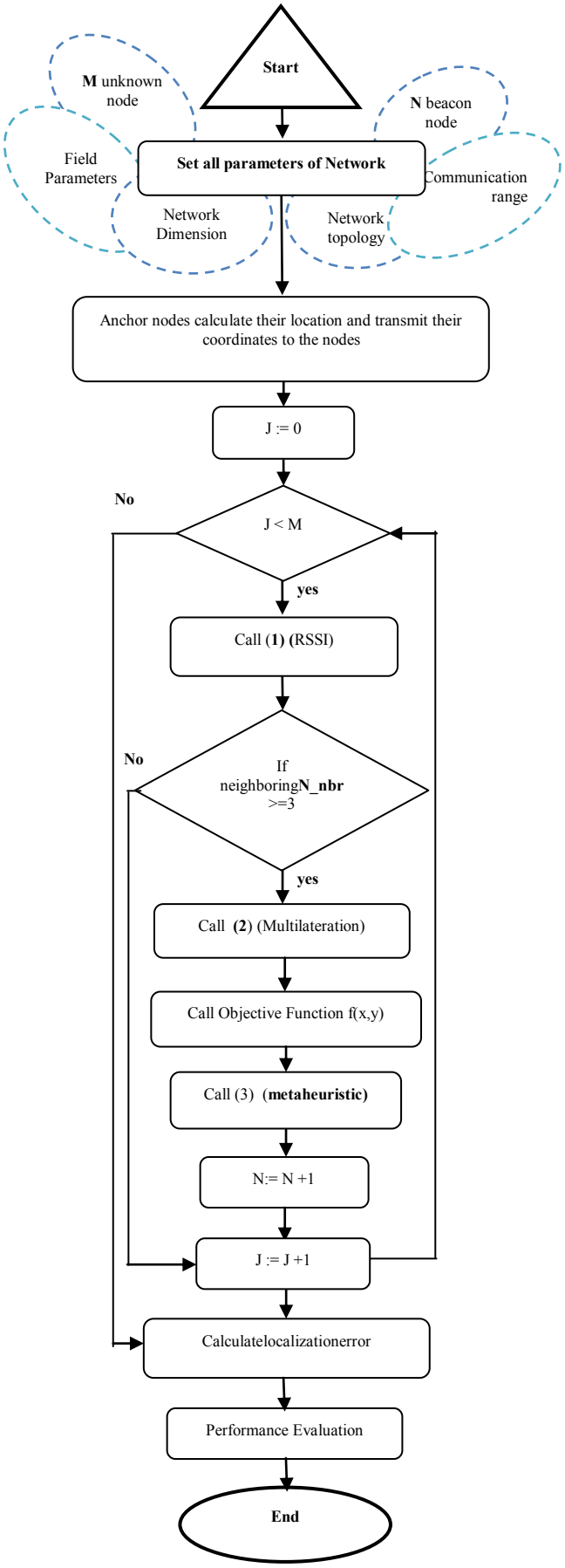


Fig.4: Flowchart of node localization

V. SIMULATION EXPERIMENTS AND PERFORMANCE EVALUATION

A. Simulation Experiments

Two major metrics [19] are proposed for performance evaluation:

1) **Average Location Errors (ALE):** This is equal to average distance between the estimated location (x_i, y_i) and actual location (X_i , Y_i) of all sensor nodes.

$$E_L = \frac{1}{M_L}\sum_{i=1}^{L}\sqrt{(x - X_i)^2 + (y - Y_i)^2}$$

2) Average Execution Time (AET): *which is the average time required for localization of all sensor nodes*

$$Average\ excution\ time = \frac{\sum_{i=1}^{n} excution\ time}{n(number\ of\ sensor\ node)}$$

The total nodes example are deployed in Fig. 5 , the C-shape of the area is selected for the first deployment , where in the first picture 400 nodes are deployed randomly , 0,2 % are anchors nodes and 0,8 are the target nodes .

The main objective is to find out the location of the 0.8 % unknownnodes by the meta-heuristic localization algorithm

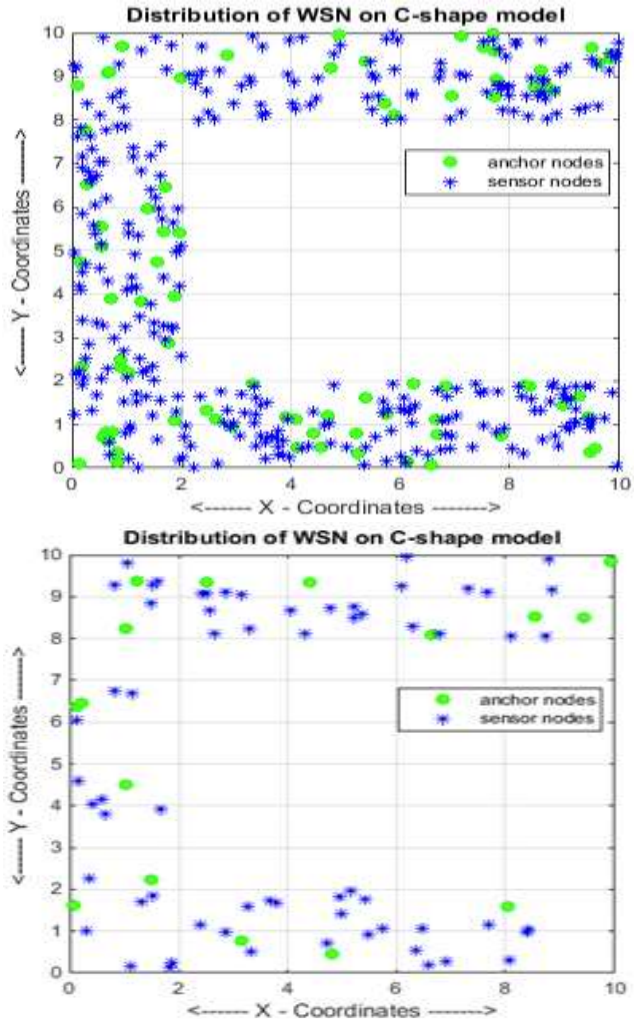


Fig.5: network deployment in C-shape

The second example are deployed in Fig.6 , the square shape of the area is selected for the first deployment , where in the first picture 400 nodes are deployed randomly , 0,2 % are anchors nodes and 0,8 are the target nodes .

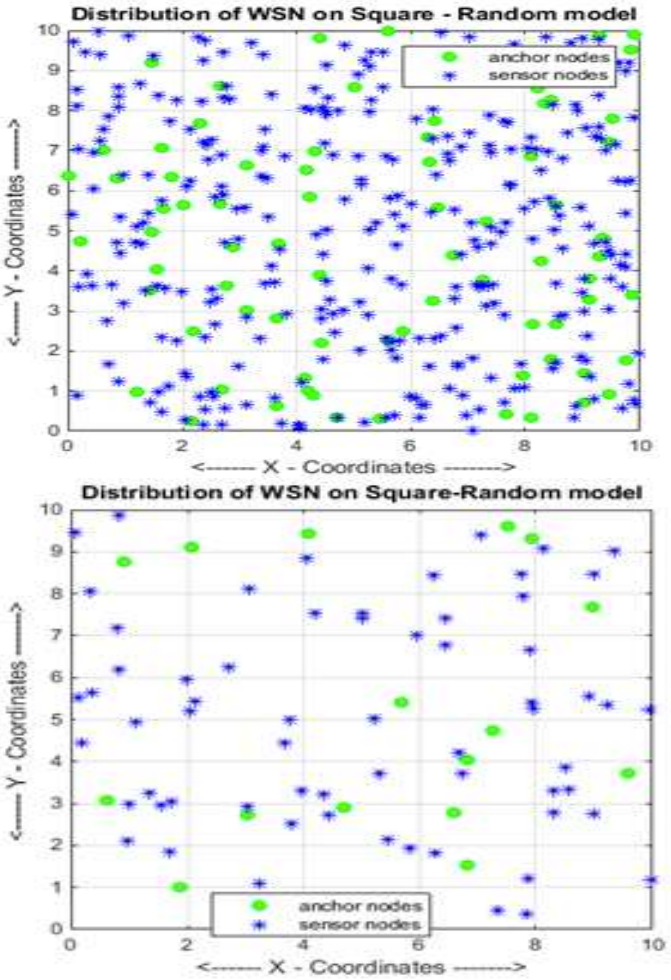


Fig.6: deployment of the network in Square- Random

B. Performance Evaluation

The same configuration of the network is simulated for the three algorithms PSO, HPSO,BPSO.

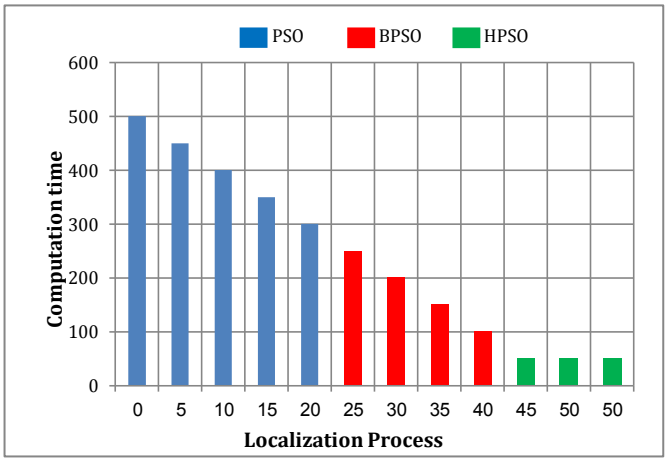


Fig.7: computation time required during localization

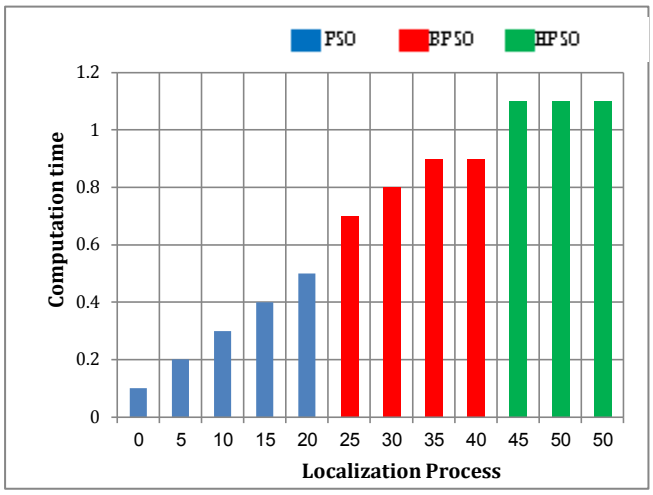


Fig.8: localization Error obtained during localization

From Fig. 7, we show that HPSO converge quickly than the two others, but in the fig. 8, we found that the localization error of original PSO gives more accuracy then the two others algorithms.

The interpretation of this difference focuses on the variation between the exploration and exploitation, where the exploitation consists of probing a limited region of the search space with the hope of improving a promising solution K that we already have at hand. This operation amounts then to intensifying (refining) the search in the vicinity of K, on the other hand, the exploration consists of probing a much larger portion of the search space with the hope of finding other promising solutions that are yet to be refined. This operation amounts then to diversifying the search in order to avoid getting trapped in a local optimum.

VI. CONCLUSION

Wireless sensor networks are extensively used in most of the areas of modern world intelligent applications. Most of these applications demand location information of the sensor nodes.

In this paper node localization challenge is treated as multidimensional optimization, and three variant of Particle Swarm Optimization are evaluated under two important criteria the performance evaluation (localization error and computing time) are addressed in this paper among the three variants approach of PSO.

To balance between the exploration and exploitation phases is was a delicate task where the first one converge and the other diverge at the same time. This task makes the operation very difficult to be realized.

The future objective is focalized to add energy consumption as third criteria for performance evaluation of node localization in a wireless sensor network, on the other hand ,hybridization with other algorithms may also prove to be fruitful. , we will extend the scheme to counter different types of malicious attacks in sensor localization without incurring too much additional computational cost and communication overhead and apply it to different network environments to further verify and improve the accuracy of sensor localization in hostile or untrusted environments.

REFERENCES

[1] M. A. Adnan , M. A. Razzaque, I. Ahmed , I. F. Isnin ,“ Bio-Mimic Optimization Strategies in Wireless Sensor Networks: A Survey ” , Sensors, vol 14,pp. 299-345, 2014

[2] [I.F.Akyildiz,W.Su,Y.Sankarasubramanium, E.Cayirci, “Wireless Sensor Networks: A Survey”, IEEE Communication Mag , vol. 40, pp. 102 –114,2002

[3] K.Sohraby,D.Minoli,T.Znati, “ Wireless sensor networks: Technology, protocols, and applications”,Book ,Wiley,London2007.

[4] N. A. Alrajeh,M. Bashir,B.Shams,“ Localization Techniques in Wireless Sensor Networks ”, International Journal of Distributed Sensor Networks , Vol. 2013, Article ID 304628,9 page .

[5] T.J.S.Chowdhurya,C.Elkin, V.Devabhaktuni,D. B.Rawat, J.Oluoch, “ Advances on Localization Techniques forWireless Sensor Networks: A Survey ”,Computer NetworksVol. 110, pp. 284-305, December 2016.

[6] A. Pal , Localization Algorithms in Wireless Sensor Networks: Current Approaches and Future Challenges , Network Protocols and Algorithms , Vol. 2, pp. 45-73, March 2010 .

[7] G. Han, H.Xu, T. Q. Duong, J. Jiang, T. Hara ,“ Localization algorithms of Wireless Sensor Networks: a survey ” ,JournalTelecommunications Systems ,Vol .52 , pp. 2419-2436 , April 2013.

[8] Q. T. Hoang , T. N. Le , Y. Shin, “An RSS comparison based Localization in Wireless Sensor Networks” , 8th workshop on Positioning Navigation and communication WPNCApril 2011.

[9] J. Cheon, H.Hwang, D. Kim, Y. Jung , “ IEEE 802.15.4 ZigBee-Based Time-of-Arrival Estimation for Wireless Sensor Networks “,Sensors , v.16 , Feb2016 .doi:10.3390/s16020203 .

[10] G. Zhu ,J. Hu , “ A distributed continuous-time algorithm for network localization using angle-of-arrival information ” ,Automatica ,Vol .50, Issue 1, pp. 53-63, January 2014 .

[11] PK. Singh, B.t Tripathi, N. P. Singh,” node localization in wirless sensor network ”, International Journal of Computer Science & Information Technology , vol . 26 , 2568-2572 , 2011.

[12] A .Singh , S .Kumar ,O . Kaiwartya , A Hybrid Localization Algorithm for Wireless Sensor Networks ,Procedia Computer Science ,Vol. 57, pp. 1432-1439 , 2015 .

[13] A. Boukerche, H. Oliveira, E. Nakamura, and A. Loureiro, “Localization systems for wireless sensor networks”, IEEE wireless Communicationsb,Vol . 146 , pp. 6–12, 2007 .

[14] A. Gopakumar , L. Jacob, “Localization in wireless sensor networks using particle swarm optimization” , International Conference on Wireless, Mobile and Multimedia Networks, Beijing, China , 227–230, 2008.

[15] R. Kulkarni, G. Venayagamoorthy, M. Cheng, “Bio-inspired node localization in wireless sensor networks”, International Conference on Systems, Man and Cybernetics, , 205–210,2009.

[16] I. F. M. Zain, S.Y.Shin ,” Distributed Localization for Wireless Sensor Networks using Binary Particle Swarm Optimization (BPSO) ” , IEEEVehicular Technology Conference , May 2014 .

[17] A. Kumar, A. Khoslay, J.S. Sainiz, S. Singh ,” Meta-Heuristic Range Based Node LocalizationAlgorithm for Wireless Sensor Networks” ,International Conference onLocalization and GNSS (ICL-GNSS), IEEE, June 2012.

[18] D. Chandirasekaran, T. Jayabarathi,” A Case Study of Bio-Optimization Techniques forWireless Sensor Network in Node Location Awareness” , Indian Journal of Science and Technology, 2015 , Vol. 8 , November 2015 .

[19] F.Abdi, A. T. Haghighat, “ a hybrid rssi based localization algorithm dor wsn using a mobile anchor node”, International Conference on

Two new Quantum Attack Algorithms against NTRU_pke # KA_NTRU # & # PA_NTRU #.

1st LAAJI EL Hassane
ACSA Laboratory
Mohammed First University
Oujda, Morocco
e.laaji@ump.ac.ma

2nd AZIZI Abdelmalek
ACSA Laboratory
Mohammed First University
Oujda, Morocco
abdelmalekazizi@yahoo.f

3rd AZZOUAK Siham
ACSA Laboratory
Sidi Mahammed Ben Abdellah University
Fes, Morocco
sezzouak@gmail.com

***Abstract*—The NTRUencrypt authors submitted four versions to National Institute of Standardization(NIST) competition since 2016 and it is still in process for the second round. The NTRU_pke release is one of them, it is defined in the ring $\mathbf{R_q} = \mathbb{Z}_q[X]/(X^n-1)$; and the private keys and the plaintext are codified in trinary polynomial, that means all their coefficients are in {-1,0,1}.**

Our two quantum attacks algorithms KA_NTRU and PA_NTRU on NTRU_pke implementation, inspired from Grover's Algorithm, targeted respectively to find Private Keys and Plaintext. For testing the implementation attacks, we create a NTRU_pke test version named NTRU_Attacks. In the general case, the quantum algorithms can break a system of dimension n in $2^{n/2}$ time.

***Index Terms*—NTRU, NewHope, Lattice- Based-Cryptography, Post Quantum cryptography, Grover' Algorithm.**

I. Introduction

The big concern of the cryptographic community now, is to build new cryptosystem Post-Quantum cryptosystems able to resist against these attacks, because the near future the cryptosystems used right now like RSA, ECDH, El Gamal will be easily broken the quantum computer using quantum algorithms like Grover's algorithm, Shor's algorithm or others "Quantum computer using a quantum algorithm can solve a problem of dimension n in $2^{n/2}$ time "[1].

This is why the National Institute of Standards and Technology(NIST) launch a competition since 2016 and it is still in process for choosing one or more post-quantum cryptosystems [2]. The authors of NTRUencrypt submitted four schemes NTRU_PKE (Public Key Encryption) NTRU_KEM (Key Exchange Mechanism) ss-NTRU_pke and ss-NTRU_kem. Our focus in this work on NTRU_pke as described by the authors, it is based on the original NTRU with new parameters [3] that achieves CCA-2 security via NAEP transformation [4]. It is amongst the most important Lattice-Based submissions to the NIST competition [3]. It uses the hardest problems on points lattices in $\mathbb{R}^n$ like SVP (Short Vector Problem) and CVP (closet Vector Problem). the NTRU assumption is defined by:" Having $h = g/f$ it is hard to find f and g. The NTRU assumption can be reduced to the *uSVP* for the NTRU lattices". The NTRU has survived for 20 years of cryptanalysis, and judged to be able to resist against quantum attacks, and deemed able to take over and take the place of classical cryptography.

A. Related works:

The most attacks used to check the robustness of Lattice-Based Cryptosystems are the Reduction algorithms attack and Meet-In-the-Middle (MIM) attack developed by (Oldgz) [4], or the hybrid attacks that use the mixture of the reduction attack and MIM attack [5]. Others types attacks exist like Cold Boot attack developed by Martin Albrecht et.al.[6] and another aspect of security problems named Side-channel attack developed by Kocher [7].

B. Our work

In this paper, we present two attacks algorithms on NTRU_pke implementation level, named **KA_NTRU** and **PA_NTRU** targeted respectively to find the private keys and plaintext. The domain of NTRU_pke is the ring $\mathbf{R_q} = \mathbb{Z}_q[X]/(X^n-1)$, and the private keys are trinary polynomials generated according to Uniform Distribution, that means that all their coefficients are in {-1,0,1} and the plaintext also codified in a trinary polynomial. For testing our attacks, we re-implemented new release NTRU_Attacks which include the attacks implementation functions. For example, we tested the attacks with small polynomial dimensions, we obtained the bellow result: when the polynomial dimension is equal to 17 the system was broken in about 1,5 minutes for KA_NTRU and in about 30 seconds for PA_NTRU. All our test is performed in computer PC Toshiba i7. And we note that our work is inspired from Grover's algorithm and Scott Fluhrer work[8]. The NTRU_pke scheme chooses all the trinary polynomials according to a Uniform Distribution (UFD), indeed, an attacker can use the Quantum Computer and our attacks to break the system by sampling simultaneously the coefficients of the trinary polynomials to find respectively the private keys and plaintext as we are going to describe in section 5.

C. Outline

The remainder of our work is organized as follows:

Section 1: this introduction;

Section 2: preliminaries: We start by noting and defining the terminology used in this paper. Then we recall the necessary knowledge of the Lattice-Based-Cryptography, a brief description of sampling methods Uniform distribution (UFD) and we also give a brief description of quantum algorithms.

Section 3: We recall the related work's description of the

principal attacks on NTRU cryptosystem.
Section 4: We give an overview of the original NTRU scheme and NTRU_pke release submitted to NIST competition;
Section 5: We present our two attacks algorithms KA_NTRU and PA_NTRU against NTRU_pke to recover respectively the private keys and the plaintext.
Section 6: In this section, we present the principal specification of our attacks, implementations and our new release implementation NTRU_Attacks.
Section 7: We draw conclusions and some topics that may provide interesting research area.

II. PRELIMINARIES

A. Notations

In the remainder of this paper, we use the following notations: LBC for Lattice-Based-Cryptography[9]; $L_{(B)}$ Lattice of $\mathbf{R}^n$ with base $\mathbf{B} = (\vec{e_1}, ..., \vec{e_n})$ with the form $\mathbf{L}_{(B)} = \{ \vec{v} \in \mathbb{R}^n, (a_1, ..., a_n) \in \mathbb{Z}^n$ et $\vec{v} = a_1\vec{e_1} + ... + a_n\vec{e_n}\}$[3]; $\mathbf{R} = \mathbf{Z}[X]/(X^n - 1)$ the ring polynomial with coefficient in $\mathbb{Z}^n$; and R_q the quotient ring polynomial with coefficients in [0 , q]; $\|\vec{v}\|$ the norm of vector $\vec{v}$; $\|\vec{v}\|_s = max|v_i|$ the low-norm ; **(a,b,..)** uppercase the elements of **R**; (a,b,...) lowercase the coefficients of elements of **R**; the $< \vec{v}.\vec{u} >$ inert product of$\vec{v}$ and $\vec{u}$; we refer to sampUFD(seed) the polynomial sampled according to Uniform Distribution . We refer to *Trinary Polynomials*
$T(d_1, d_2) = a(x) \in R$ with the polynomial*a(x)* has d_1 coefficients equal to *1*; d_2 coefficients equal to -1 and the rest of coefficients equal to *0*.
We refer to **KA_NTRU** the Private Key Attack algorithm, we refer to **PA_NTRU** the Plaintext Attack Algorithm and the we refer to **NTRU_Attacks** Our test implementation release of the original cryptosystem NTRU_pke which takes into consideration our idea and keeps all the parameters[5].

B. Lattices Problems

LBC like all cryptosystems it is based on mathematical concepts and theories to encrypt and decrypt as well as to demonstrate the complexity and the difficulty of breaking those cryptographic systems by posing problems that are difficult to solve. The principal Lattice problems are SVP and CVP and their approximate versions. *The Shortest Vector Problem (SVP)*[9]: Finding (SVP) in Lattice $L_(B)$ is finding a nonzero vector that minimizes the Euclidean norm. Formally the problem SVP is to find a non-zero vector:

$$\tilde{\mathbf{v}} \in \mathbf{L_{(B)}} forall \tilde{\mathbf{x}} \in \mathbf{L_{(B)}} wehave \|\tilde{\mathbf{v}}\| \leq \|\tilde{\mathbf{x}}\| \qquad (1)$$

The Closest Vector Problem (CVP): Given the Lattice $L_{(B)}$, and a vector $\tilde{\mathbf{w}} \in \mathbf{R^m}$ to find a vector $\tilde{\mathbf{v}} \in \mathbf{L_{(B)}}$ "Closest" to $\vec{w}$, is to find a vector$\vec{v} \in L_{(B)}$ that minimizes the Euclidean norm $\|\vec{w} - \vec{v}\|$ where:

$$\|\vec{w} - \vec{v}\| = \mathbf{min}\{\|\vec{w} - \vec{v}\| / \tilde{\mathbf{v}} \in \mathbf{L_{(B)}}\} \qquad (2)$$

C. LBC Cryptosystems

There are different cryptosystems based on LBC the first construction was created by AJTAI-DWORK[10] in 1996 but in 2001 Nguyen and Stern broke this cryptosystem by solving the SVP and CVP. Also, Goldreich Goldwasser and Halevi (GGH) in 1997 are created, their cryptosystem, but also in 2001 Nguyen and Stern broke this cryptosystem by solving the SVP and CVP [10] and others cryptosystems exist like Learning With Errors (LWE) created by Oded Regev in 2005 but it is still of research stage right now. Only NTRU(standardized by IEEE P1363.1 on April 2011) is judged able to resist against all attacks conjectured [11].

D. Description of Uniform Distribution law(UFD)[12]

Definition: Let **X** be a random variable on $(\omega, P(\omega), P)$ on image space: $X(\omega) = \{x_1, x_2, ..., x_n\}$ of law *p*. We say that **X** is uniform variable or **X** follows a Uniform law :

$$if \quad \forall\, i \in \{1, 2, ..., n\} \quad p(x_i) = \frac{1}{n} \qquad (3)$$

Properity: **X** being a uniform variable of image space $X(\omega) = \{x_1, x_2, ..., x_n\}$ we have Esperance $E(X) = \frac{1}{n}\sum_{i=1}^{n} x_i$ and the variance $Var(X) = \frac{1}{n}\sum_{i=1}^{n} x_i^2 - \frac{1}{n^2}(\sum_{i=1}^{n} x_i)^2$

E. Quantum Algorithm

Quantum algorithm Definition: The information in a quantum computer is in a superposition of states, therefore, the quantum algorithm performs simultaneously multiple treatments. The majority of quantum algorithms (like Shor ́s and Groveŕs algorithms) is defined by three steps consecutive:

1) The creation of a configuration in which the amplitude of the system is in any of the 2^n basic states of the system are equals;
2) The Walsh-Hadamard transformation operations (is an example of a generalized class of a Fourier transform); transform *N* qubits initialized with $(|0>)$ into a superposition of all 2^n orthogonal states expressed in the base $(|0> |1>)$ with equal weighting [13].
3) The selective rotation of different states. When a classical algorithm finds an element in a list of *N* randomly selected elements with a probability of $\frac{N}{2}$, the quantum algorithm of Grover does so with a probability of $O(N^{\frac{1}{2}})$.

F. Groveŕ's Algorithm Principle

1) Problem: Search some solutions in an unstructured database ;
2) Classical: Essential problem N entries —¿ in average $N/2$ tests;
3) Quantum Groveŕ algorithm:$O(N^{1/2})$ In general can speed up all classical algorithms using a search heuristic.
4) Formulation of the problem: *N* elements indexed from *0* to *N-1*,$N = 2^n|U>x$ search register elements repertories via their index;

The search problem admits M solutions (For more detail the reader can see [13]).

III. Related Works

Many cryptanalysis works are performed, their principal goal was to check the robustness of the Lattices cryptosystems. Others works exist for cryptosystems analysis like cold boot attack and side-channel attack as we are going to describe them in this section.

The best tools used to prove the security and the efficiency of an LBC is Hybrid Attack combined with Lattice reduction attack with LLL(Lenstra, Lenstra, Lovasz) and BKZ2 (Blockwise-Korkine-Zolotarev) and Meet-in-The-Middle attack(MIM) developed by (Odlgzko)[4].

In the NIST-2018 benchmarking realized by Albrecht et al. the authors claim that NTRUencrypt [14] warrant 198-bit security level against quantum attack and more than 256 bits of classical security.

A. Lattice Reduction

The reduction of Lattice Basis is very important, and the SVP or CVP will be easier to solve with a reduced Basis. The most reduction algorithms used to solve those Lattices problems are the LLL algorithm, BKZ.

*LLL : Lestro-Lenstra-Lovasz Algorithm:*The role of the LLL algorithm is to transform a Bad Basis $B = (\vec{e_1}, ..., \vec{e_n})$ to a Good Basis $G = (\vec{u_1}, ..., \vec{u_n})$ of a Lattice $\mathbf{L_{(B)}} \subset \mathbb{R}^{\mathbf{n}}$. It allows approximating the smallest vector in polynomial times. This can provide a partially satisfactory answer to the problems Lattices SVP and CVP on which the security of the Lattices cryptosystems is based on. [15]

Definition: The basis of a Lattice is said to be reduced by the LLL algorithm if it is obtained by the Gram-Schmidt algorithm and satisfies the following two properties:

$$\forall 1 \leq i \leq n, j < i \quad |\lambda_{i,j}| \leq \frac{1}{2} \quad |\lambda_{i,j}| = \frac{|\vec{e_i}.\vec{u_j}|}{\|\vec{u_j}\|^2} \tag{4}$$

$$\forall 1 \leq i \leq n \quad \delta.\|\vec{u_i}\|^2 \leq \|\lambda_{i+1j}\vec{u_i} + \vec{u_{i+1}}\|^2 \quad \delta \in [\frac{1}{4}, 1] \tag{5}$$

BKZ Algorithm: The main goal of BKZ is to output a BKZ-reduced basis $G_{bkz} = (\vec{u_1}, ..., \vec{u_n})$ with block size $B_{[j,min(j+\beta-1,n)]}$, with $\beta \geq 2$ and factor $\varepsilon > 0$ from reduced LLL-reduced basis. $B_{[j,min(j+\beta-1,n)]}$ is obtained by iteration reduction for $j = 1\ to\ n$, until finding the block with the SVP in the projected lattice. For more detail of this algorithm, see the Yuanmi Chen et.al work [16].

B. Meet-in-the-Middle Attack:

The goal of a general Meet-In-the-Middle attack, is to find specific elements x, x' in a search space of which it is known that $f_1(x) = f_2(x')$ search x, x' values ; the unique solution is called the golden collision; Having the private key decomposed into: $f = f + f_2$ with $f_1(deg = \frac{n}{2} - 1)$ and $f_2(deg \in [\frac{n}{2}, n - 1])$

$$h = (f_1 + f_2)^{-1} * g \Longrightarrow f_1 * h = g - f_2 * h \tag{6}$$

All rotations of the keys f and g will be a solution to this equation. Search with (almost) equal number of ones; For more description of this attack see the paper Choosing Parameters for NTRUencrypt[5].

C. Cold Boot Attack:

This attack is firstly described by Halderman et al [6]. This attack consists of the fact that bits in RAM save their value for some time after power is cut, to explore this and retain a *p0 = 1%* bit-flip, the memory must have a cold temperature at about *(-50 C°)* to retain bits for $10mn$ after computer power down. Halderman et al. also noted that " bit-flip rates as low as p0 = 0.17% are possible when liquid nitrogen is used for cooling".

D. Side-channel Attack:

The work realized by Zhe Liu et al.[7] and the work realized by Nadia El Mrabet[17], explain the side-channel attack allows the attacker to find the private keys, with the measurement of the times performing and energy consumption, or current intensity by intercepting their variations. To prevent this attack it is possible to add fictive operations for redressing (correlation of power) consumption. The main idea is to find witch fictive operation to add in each cryptographic function.

IV. NTRUencrypt

A. Overview of NTRU

It was created in 1996 by the three mathematicians J. Hofstein J. Pipher and J. H. Silverman and published in 1998 [9]. It is the first cryptosystem that is completely LBC. Its domain of computation is the ring of the polynomials $mathbf R_q = \mathbb{Z}_q[X]/(X^N - 1)$ where N is a prime number. The major advantages of using a ring structure are a relatively smaller key size and faster speed that can be achieved. NTRU consists of two protocols the NTRUEncrypt Protocol and the NTRUSign Signature Protocol. NTRU was considered reliable, by the IEEE P1363.1 standard and in April 2011 NTRUEncrypt was accepted in the X9.98 standard[9].

In terms of security, NTRU was resisted for 20 years of cryptanalysis. Its low memory consumption allows us to use it for applications such as mobile devices or smart cards.

B. NTRU schemes submitted to the NIST competition

The NTRUencrypt team [3] submitted four schemes:

1) NTRU_pke and NTRU_kem with the sequence parameters is $\{N = 443, q = 2048, p = 3, d = 143\}$ and $\{N = 743, q = 2048, p = 3, d = 247\}$, for those schemes, all the polynomials are sampled according to a Uniform Distribution (UFD) with the polynomial coefficients are in {-1,0,1}.
2) ss-NTRU_pke and ss-NTRU_kem releases with the sequence parameter $\{N = 1024, q = 1073750017, p = 2, \sigma = 724\}$ where σ is the standard deviation, and for those schemes, all the polynomials are sampled according to Discrete Gaussian distribution (DGD) or Deterministic Discrete Gaussian Distribution (DDGD).

C. NTRU_pke Description

Our work focused and concern only the NTRU_pke schemes with the parameters set warrant quantum security level 84 bits and 159 bits claimed by NIST [3]. To explain more clearly our purpose and presenting easily our work, we are going to describe the principal cryptographic functions of NTRU_pke cryptosystem. For more detail, the reader can see the authorsٌ original document[3] available in the NIST competition web site.

a) Parameters: : As described in [3] The domain of NTRU_pke is the quotient Ring with: $\mathbf{R} = \mathbb{Z}[X]/(X^N - 1)$ and $\mathbf{R_q} = \mathbb{Z}_q[X]/(X^N - 1)$. These schemes require a function that generates the trinary polynomials according to a Uniform Distribution (UFD) with *seed* sampled with **Salsa20** based pseudo-random number, the authors state that Salsa20 is 5 times faster than AES. We note that NTRU_ pke takes the private key F in the form $F = p * f + 1$ [16]. This form allows us to avoid to calculate the inverse of *f mod p* because $F = p * f + 1 \pmod p = 1$. For the actual parameters the reader can see [5].

D. NTRU_pke Algorithms

a) ***Algorithm 1: Keys Generation****:* .

Input : the sequence parameters $\{N, q, p, d\}$ and *seed*.

1) *f ,g* ← *sampUFD(seed)*; as Trinary Polynomials;
2) *F* ← *p*f+1)*;
3) F_q ← *inverse(F) mod q*;
4) $h \leftarrow g * F_q \pmod q$;

Output: the public key *h* and the private key *F* and *seed*.

b) ***Algorithm 2: Encryption*** *:* .

Input: The public key *h*, the message with its length *msg,len*, and the *seed*.

1) *M* ← *choosing* $\in \{-1, 0, 1\}$;
2) *r* ← *sampUD(rseed)* ;
3) *e* ← *sampUD(eseed)* ;
4) $c \leftarrow p * r * h + m \pmod q$;

Output: The ciphertext c.

c) ***Algorithm 3: Decryption*** *:* .

Input: The private key *F* and the ciphertext *c*.

1) *M* ← $F * c \pmod q$;
2) *M* ← *lift M* $\in \{\frac{-q}{2}, \frac{q}{2}\}$;
3) *M* ← $M \pmod p$

Output: the message *M*.

V. Our Contribution

As we described before in the abstract and the introduction sections, our quantum attacks algorithms **KA_NTRU** and **KA_NTRU** aims to break the NTRU_pke cryptosystem by finding respectively, the private key and the plaintext. An attacker with a quantum computer can use our algorithms by sampling simultaneously the polynomial coefficients respectively, of *f* and of *r* until breaking the system. We describe both algorithms as follow:

A. Our Attacks Algorithms description

a) ***Algorithm 4: KA_NTRU*** *:* .

Input: the public key *h*, the modulus *q*, and *n*

1) *Repeat :*
2) *f'* ← *sampUD(seed)* ;
3) *F'* ← *p*f'+1)*;
4) *g'* ← $F' * h \pmod q$;
5) *if* $g'_i = q - 1 \rightarrow g'_i = -1$;
6) *Until :* $g' \in \{-1, 0, 1\}$;

Output : $f = f' \quad and \quad g = g'$.

Comment: For the algorithm.4 **KA_NTRU** the attacker samples simultaneously the polynomial coefficients of *f'* (line 2) and computes $g' = F * h \pmod q$ (line 4) until the coefficients of *g'* are in {-1,0,1} (line 6) then he finds the private keys $f = f'$ and $g = g''$. We note that if a coefficient polynomial equal to $q - 1$ we must replace it by (-1) as in line 5.

b) ***Algorithm 5: PA_NTRU*** *:* .

Input: the public key *c*, the modulus *q*, and *n*.

1) *Repeat :*
2) *r* ← *sampUFD(seed)* ;
3) *c'* ← $p * r * h \pmod q$;
4) *M'* ← $c - c' \pmod q$;
5) *if* $M'_i = q - 1 \rightarrow M'_i = -1$;
6) *Until :* $M' \in \{-1, 0, 1\}$

Output : The plaintext $M = M'$.

Comment: the same for the algorithm.5 **PA_NTRU**, the attacker samples simultaneously the polynomial coefficients of *r*(line 2) and computes a polynomial $c' = p.r * h \pmod q$ as in line 4 and computes a $M' = c - c' \pmod q$ (line 5) until the coefficients of polynomials *M'* are in {-1,0,1} as in line 6, then he finds the plaintext $M = M'$. We noet that if a coefficient polynomial equal to $q - 1$ we must replace it by (-1) as in line 5.

B. Result

In this subsection, we present the result obtained by using our NTRU_attacks release implementation. Unfortunately, we haven't a quantum computer, then we are going to try our algorithms in a classical computer with small parameters just for having an idea of the speed performance of both attack algorithms. The algorithms generate trinary polynomials with parameters *d* the number of coefficients in trinary polynomial equal to (1) and equal to (-1) chosen respectively in { 2,3,4,5,6} , the dimension *n* chosen respectively in {7,11,13,17,19} and we chose also small modulus $q = 127$. In the **table1** we give the cost of the KA_NTRU attack to find the private keys and in the **table2** we give the cost of PA_NTRU attack to find the plaintext.

TABLE I
Cost of KA_NTRU attack against NTRU_pke

Attacks	n:7	n:11	n:13	n:17	n:19
Times(ms)	46	69	$4{,}7.10^3$	98.10^3	$3. .10^6$
Operations	346	690	95.10^3	$2{,}3.10^6$	$5{,}6.10^6$

TABLE II
COST OF PA_NTRU ATTACK AGAINST NTRU_PKE

Attacks	n:7	n:11	n:13	n:17	n:19
Times(ms)	5	1,5 $.10^3$	3.10^3	29.10^3	51.10^3
Operations	54	35.10^3	65.10^3	662.10^3	10^6

VI. IMPLEMENTATIONS

Our implementation of KA_NTRU algorithm and PA_NTRU algorithm and ours NTRU_Attacks were implemented on C++ and performed in PC-TOSHIBA –Satellite, Processor Intel, Core™i7 -2630QM CPU, 2GHz, RAM 8 GO, under environment Windows 7-32 bits and Dev-C++ 4.9.9.2.
For NTRU_Attacks we keep all the parameters and the reference implementation functions of NTRU_pke, with few modifications. , specially we re-used the reference implementation of " *void trinary_poly_gen(rr,d,n);* " function for sampUFD as described in the algorithms.

For the ploynomials multiplication we not used the **Karashuba** algorithm as in NTRU_pke release submitted to NIST, we used our own polynomlials multiplication *XKwarizm* algorithm in the ring $\mathbf{R_q} = \mathbb{Z}_q[X]/(X^N - 1)$, in our paper under title N̈ew Multiplication Algorithm +600% faster than NTT algorithm when applied to NTRU1024s̈ubmitted to J̈ournal of Cryptographic Enginneringön mars-2019 "unpublished" [19], the reader can see the *XKwarizm* algorithm in [Appendix A].
For testing the KA_NTRU and PA_NTRU attacks algorithms, we integrate their implementation functions in
NTRU_Attacks as follow:

- The program performs the keys generation function and encryption function and checks the decryption function;
- The *KA_NTRU(.)* function receives the public key *h* and returns the private keys *f, g*;
- The *PA_NTRU(.)* function receives the ciphertext *c* and returns the plain text *m*.

Note: All source implementations of those attacks are available into the website at : Sources Code or the reader can contact us at: *e.laaji@ump.ac.ma*.

VII. CONCLUSION

The evolution in quantum computer science is very fast, whereas the choice of PQcryptosystem for standardization is in the NIST process, to prepare for a smooth migration of classical cryptosystems to post-quantum cryptosystems [2]. We are not sure that some cryptosystems submitted will be resistant against quantum attacks. It is possible to modeling our algorithm attacks and apply them to some others Lattice-based submissions to NIST inspired from original NTRU schemes like NTRUprime [20] or R-LWE (Ring Learning With Error) schemes like NewHope [21]. For example, to apply **KA_NTRU** Attack to NTRUprime, the attacker can generate simultaneously a polynomial f and computing $3 * h * f = g \pmod q$ until the coefficients of g are in {-1,0,1}
. The same for New Hope implementation, the hardness assumption is defined by: " Having $b = a * s + e$, it is hard to find s". Therefore an attacker can sample a polynomial s and computes $b - as = e \pmod q$ until the polynomial coefficients of e are in{0,1} or in{0,1,2,3 } according to the choice of error area and then return the private key s. A lot of researchers in this cryptographic domain said that " only Quantum Cryptography will resist against Quantum Attacks ", but we continue our work on the cryptanalysis and improvement of the post-quantum cryptosystems and we hope to contribute with all cryptographic community to build the strong cryptosystems to save the private life of the person by learning from the best actual practices and innovate new methods.

REFERENCES

[1] Christine van Vredendaal. Available at "http:photon.physnet.uni-hamburg.defileadminuser_uploadILP"
[2] Lily Chen,StephenJordan,Yi-Kai Liu,Dustin Moody ,Rene Peralta ,Ray Perlner ,Daniel Smith "NISTIR 8105- Report on post-quantum cryptography", Tone –Avril 2016.
[3] Cong chen, Jeffrey hHoffstein and al., "NIST PQ submission: NTRUencrypt a lattice-based encryption algorithm", Brown University and Onboard security Wilmington USA
[4] Christine van Vredendaal, " Reduced memory meet-in-the-middle attack against the NTRU private key"
[5] JeffHofstein1, Jill Pipher1, John M. Schanck, Joseph H. Silverman1, William Whyte, and Zhenfei Zhang , "Choosing Parameters for NTRUencrypt", Brouwn University USA, Security Innovation Wilmington USA.
[6] Martin R. Albrecht, Amit Deo and Kenneth G. Paterson, "Cold boot attacks on ring and module LWE Keys under the NTT" , Royal Holloway, University of London.
[7] Zhe Liu et al. "FourQ on embedded devices with strong countermeasures against side-channel attacks" University of Waterloo, Canada
[8] Scott Fluhrer , "Quantum cryptanalysis of NTRU- cisco systems", July 5, 2015
[9] J.Hofstein, J. Pipher, and J. H. Silverman, " Introduction Mathematics and Cryptography, NTRU" , 1998
[10] Michael Hartmann," Ajtai-Dwork cryptosystem and other cryptosystems based on lattices". Universite de Zurich,29 October 2015
[11] Daniele Micciancio, OdedRegev ," Lattice-based cryptography", July 22, 2008
[12] Dupont , Fleury . "Probabilités ". Vibert prépa, pp 44 – 45 . mars 1986
[13] Colin P. Wiliams , "Grover Algorithm Explorations in Quantum Computing", Springer 2011
[14] Martin R. Albrecht, Benjamin R. Curtis B and al. ," Estimate all the fLWE, NTRU schemes" , Version: May 2, 2018
[15] Chris Peikert, " Lattice cryptography for the Internet", July 16, 2014
[16] Yuanmi Chen and Phong Q. Nguyen . BKZ 2.0, "Better lattice security estimates", ENS Paris, 2017.
[17] Nadia El Mrabet , "Attaques par canaux caches", Université de Caen, France 2010
[18] R.Mamdikar, V. Kumar & D. Ghosh," Enhancement of NTRU public key", National Institute of Technology, Durgapur
[19] A.Azizi, H.Laaji, S.Ezzouak ," New multiplication algorithm +600 % faster than NTT algorithm when applied to NTRU1024" -XKhwarizm-, Mohammed First University Morocco 2019.
[20] Daniel J. Bernstein et al, "NTRU Prime" , Department of Computer Science- University of Illinois at Chicago, Chicago, USA 2016.
[21] Erdem Alkim, "Post-quantum key exchange,- New Hope - "Department of Mathematics, Ege University, Turkey-LéoDucas

Appendix A Our own polynomial multiplication *XKwarizm* algorithm in the ring $\mathbf{R_q} = \mathbb{Z}_q[X]/(X^N - 1)$. It allows us to multiply two polynomials *f and g* in $\mathbf{R_q} =$ and then return a polynomial h directly reduced in $\mathbf{R_q} =$.

a) ***Algorithm : Xkhwarizm*** *:* .

Input: Polynomials f *and* g , with their degrees less than *(n)*, and *modulus* q;

Output: the polynomial h.

1. Function *Xkhawarism (f,g) :*
2. . For : int $i = 0$ to $n - 1$ do :
3. ... If $f_i! = 0$ then
4. ..... For : int $j = 0$ to $n - 1$ do :
5. ..... If $g_j! = 0$ then :
6. ..... $If((i + j) < n)$ then : $h_{i+j} \leftarrow h_{i+j} + f_i.g_j$;
7. ..... else : $h_{i+j-n} \leftarrow h_{i+j-n} + f_i.g_j$;
8. .....endif(line6)
9. .....endif(line5)
10. .....endfor(line4)
11. .... endif(line3)
12. .endfor (line2)
13. For : integer $i = 0$ to n do: $h_i \leftarrow h_i \pmod q$;
14. endfunction.

Output: The result polynomial of product h;

b) Algorithm description:: In line2, the algorithm opens the first loops, it performs all instructions from index $i = 0$ *to* $i = n-1$.Then in line3, It checks, if the polynomial coefficient f_i equal to zero then return to the line2, else we perform the line3, it opens the second loops, also in line5, if the polynomial coefficient g_j is equal to zero then return to the line4. In line6, if the sum of degrees $(i + j) < n$, the algorithm computes the polynomial coefficienth_{i+j} by adding its value to the product of f_i and g_j, else $if(i+j) > n$, it computes h_{i+j-n}, in line7, by adding its value to the product of$f_i$and g_j, and finally the algorithm reduces all coefficients of the polynomial h mod q, and out put it.

Study On Skew Codes over The ring $\mathbb{Z}_q + u\mathbb{Z}_q$

1st Hebbache Zineb
Faculty of Mathematics
Univesity of Science and Technology Houari Boumedien
Algiers, Algeria
zinebhebache@gmail.com

2nd Guenda Kenza
Department of Electrical and Computer Engineering
University of Victoria
PO Box 1700, STN CSC, Victoria, BC, Canada V8W 2Y2.
ken.guenda@gmail.com

***Abstract*—In this paper, we study the properties of skew cyclic and skew negacyclic codes over the ring $R = \mathbb{Z}_q + u\mathbb{Z}_q, u^2 = 0$. We give the complete structure of skew cyclic and skew negacyclic codes. A necessary and sufficient condition for skew cyclic (skew negacyclic) codes to be free is presented. By defining a Gray map from $R = \mathbb{Z}_q + u\mathbb{Z}_q$ to $\mathbb{Z}_q^{2n}$, it has been proved that the Gray images of a skew negacyclic code of length n over R is a skew $2-$quasi negacyclic codes over $\mathbb{Z}_q^{2n}$. We prove that the Gray images of skew cyclic codes of odd length n over R with even characteristic are equivalent to a skew quasi negacyclic code of length $2n$ over $\mathbb{Z}_q$ of index 2. Further, a necessary and sufficient condition for skew cyclic (resp. skew negacyclic) codes over R that contains its dual has been given.**

***Index Terms*—$\mathbb{Z}_q + u\mathbb{Z}_q$, skew polynomial ring, skew cyclic codes, skew negacyclic codes, gray map, dual code.**

I. Introduction

Algebraic coding theory deals with the design of error-correcting and error-detecting codes for the reliable transmission of information across noisy channel. The class of constacyclic codes play a very significant role in the theory of error-correcting codes. The sub-class of constacyclic codes is negacyclic codes and were introduced by Berlekamp [6] in 1968. Then in 1999, negacyclic codes of odd lengths were generalized over $\mathbb{Z}_4$ by Wolfmann [30]. In 2003, Blackford [12] extended the results of [30]. After that in a series of papers ([3], [4], [5], [31]) studied the structural properties of cyclic codes and negacyclic codes over $\mathbb{Z}_q + u\mathbb{Z}_q, u^2 = 0$. In 2018, Bag *et al.* [2] have studied the properties of negacyclic codes over the ring $\mathbb{Z}_p + u\mathbb{Z}_p + \cdots + u^k\mathbb{Z}_p$, for odd prime p. But many of these studies are on the commutative rings. In several recent studies, generalized forms of cyclic and constacyclic codes have been investigated over noncommutative rings as skew cyclic and skew constacyclic codes respectively.

The first study of cyclic codes over noncommutative ring was discussed by Boucher *et al.* [7] In this study, they studied cyclic codes over skew polynomial ring denoted by $\mathbb{F}_q[x, \theta]$, where $\mathbb{F}_q$ is a finite field and θ is an automorphism on $\mathbb{F}_q$. One of the most important motivations of studying codes over skew polynomial rings is that the polynomials over these rings present many factorizations and because of this reason, skew polynomial rings have more advantages than commutative rings in terms of the number of ideal. Thus, studies of codes in skew polynomial rings present many new codes with better Hamming distance than any best known linear codes in literature with comparable parameters ([7], [8], [10], [18]). Furthermore, constacyclic codes have also been studied in this setting by some researchers (Boucher *et al.* in 2008, Jitman *et al.* in 2012, Sharma *et al.* and Melakhessou *et al.* in 2017). Such codes are called skew constacyclic codes. In this paper, we study the properties of $\Theta-$cyclic (resp. $\Theta-$negacyclic) code over R, where $R = \mathbb{Z}_q + u\mathbb{Z}_q$, with $u^2 = 0$, and Θ is an automorphism of R and we determined the generators of $\Theta-$cyclic (resp. $\Theta-$negacyclic) and dual $\Theta-$cyclic (resp. $\Theta-$negacyclic) codes. We have also established the necessary and sufficient condition for it to contain it's dual.

The remainder of this article is organized as follows. Results concerning skew polynomials over $\mathbb{Z}_q + u\mathbb{Z}_q$, with $u^2 = 0$, these are discussed in Section 2. In Section 3, we have presented a structure of skew cyclic (resp. skew negacyclic) codes of arbitrary length over R. We have obtained a necessary and sufficient condition for skew cyclic (resp. skew negacyclic) to be free. In section 4, the structures of the Gray images of a skew negacyclic code of length n over R are determined. In addition, if the length n is odd, the Gray images of a skew cyclic code over R with even characteristic are studied. Finally, a necessary and sufficient condition for skew cyclic (resp. skew negacyclic) code over$R$ that contains its dual is given.

II. Preliminaries

Let $R = \mathbb{Z}_q + u\mathbb{Z}_q$, where p is some prime, $q = p^m$ and $u^2 = 0$. The ring R is isomorphic to the ring $R = \frac{\mathbb{Z}_q[u]}{\langle u^2 \rangle}$ and $R = \{a + ub : a, b \in \mathbb{Z}_q\}$. It can easily be seen that the ideal (p, u) is the unique maximal ideal of R, and hence R is a local ring. But it is not a chain ring, since neither of the ideals (p) or (u) is included in each other. Further, R is not principal since the ideal (p, u) cannot be generated by any single element of this ideal.

Define a map

$$- : R \to R/(p, u)$$

$$r = a + ub \mapsto a(mod\ p).$$

The map $-$ is a ring homomorphism and $R/(p, u)$ is denoted by the residue field $\overline{R}$. Since for any $r = a + ub, a \in \mathbb{Z}_q$, then $\overline{R}$ is isomorphic to the finite field $\mathbb{F}_p$.

To define skew polynomials over R, we first give the structure of the automorphism group of R denoted by $Aut(R)$. For $\theta \in \mathbb{Z}_q$, $Aut(R)$ is given by the automorphism Θ as:

$$\Theta\colon R \to R$$

$$\Theta(a+ub)=\theta(a)+\eta(u)\theta(b)=(a+kb)+udb, \quad (1)$$

for all $a+ub\in R$. Note that an automorphism Θ in R must fix every element of $\mathbb{Z}_q$ i.e $\theta(a)=a$, and $\eta(u)=k+ud$, where k is a non-unit in $\mathbb{Z}_q$, $k^2\equiv 0\ mod\ q$ and $2kd\equiv 0\ mod\ q$.

Considering the finite ring R and automorphism Θ of R defined above, we define a ring structure on the set

$$\Re=R[x,\Theta]=\{a_0+a_1x+\cdots+a_nx^n; a_i\in R \text{ and } n\in\mathbb{N}^*\}.$$

The addition in the ring $R[x,\Theta]$ is the usual polynomial addition and multiplication is defined as follows:

$$(ax^i)(bx^j)=a\Theta^i(b)x^{i+j}.$$

The multiplication is extended to all elements in $R[x,\Theta]$ by associativity and distributivity. The ring $R[x,\Theta]$ is called a skew polynomial ring over R and an element in $R[x,\Theta]$ is called a skew polynomial. It is easily seen that the ring $R[x,\Theta]$ is non-commutative unless Θ is the identity automorphism on R.

Lemma 1: [28, Lemma 1] Let $f(x)$ and $g(x)$ be two nonzero polynomials in $\Re$ such that the leading coefficient of $g(x)$ is a unit. Then there exist unique polynomials $q(x)$ and $r(x)$ such that

$$f(x)=q(x)g(x)+r(x) \text{ where } \deg r(x)<\deg g(x).$$

According to [27] we have the following theorem.

Proposition 1: Let n be a positive integer and λ a unit in R. Then the following statements are equivalent:

i) $x^n-\lambda$ is central in $\Re$.
ii) $\langle x^n-\lambda\rangle$ is a two-sided ideal.
iii) n is a multiple of the order of Θ and λ is fixed by Θ.

A code of length n over R is a nonempty subset of R^n. A linear code C over R of length n is a $R-$submodule of R^n. In this paper, all codes are assumed to be linear unless otherwise stated.

Definition 1: A linear code C of length n over R is said to be skew constacyclic, or specifically, $\Theta-\lambda-$constacyclic if C if and only if C is invariant under the $\Theta-\lambda-$constacyclic shift operation $\rho_{\Theta,\lambda}$ where

$$\rho_{\Theta,\lambda}: R^n\to R^n$$

defined by

$$\rho_{\Theta,\lambda}(a_0,a_1,\ldots,a_{n-1})=(\lambda\Theta(a_{n-1}),\Theta(a_0),\ldots,\Theta(a_{n-2})).$$

Clearly, C is said to be skew cyclic code for $\lambda=1$ and skew negacyclic code for $\lambda=-1$. Furthermore, when Θ is the identity automorphism, they become classical constacyclic, negacyclic and cyclic codes and we denote the negacyclic shift by ρ_{-1}.

In the polynomial representation of elements of R^n, a $\Theta-\lambda-$constacyclic code of length n over R is an ideal of $\Re/\langle x^n-\lambda\rangle$. In particular for $\lambda=1$ (resp. $\lambda=-1$) a skew cyclic (resp. skew negacyclic) code is an ideal of $\Re/\langle x^n-1\rangle$ (resp. $\Re/\langle x^n+1\rangle$). Furthermore, due to Proposition 1, $\Re/\langle x^n-\lambda\rangle$ is meaningful if only if $\langle x^n-\lambda\rangle$ is two-sided, or equivalently, n is a multiple of the order of Θ and λ is a unit fixed by Θ.

For this purpose, throughout, we restrict our study to the case where the length n of codes is a multiple of the order of Θ and λ is a unit in $R^{\Theta}[x^e]$, where denotes the subring of R^{Θ} fixed by Θ.

Theorem 2.1: [27, Corollary 2] Let C be a code of length n over R and $\Theta\in$ Aut(R) with order e. Then C is $(\Theta,\lambda)-$constacyclic if and only if the skew polynomial representation of C is a left ideal in $\Re/\langle x^n-\lambda\rangle$, where λ is fixed by Θ and n is a multiple of e.

Definition 2: Let A and B be two linear codes. Then the operations $\otimes$ and $\oplus$ are defined by

$$\begin{aligned} A\otimes B&=\{(a,b); a\in A, b\in B\}\\ A\oplus B&=\{a+b; a\in A, b\in B\}\end{aligned} \quad (2)$$

Let C be a linear code over R. Then define:

$$\begin{aligned} C_1&=\{x\in\mathbb{Z}_q^n; \exists y\in\mathbb{Z}_q^n, x+uy\in C\}\\ C_2&=\{y\in\mathbb{Z}_q^n; \exists x\in\mathbb{Z}_q^n, x+uy\in C\}.\end{aligned} \quad (3)$$

It is clear that C_1 and C_2 are are linear codes of length n over $\mathbb{Z}_q$. Moreover, the linear code C of length n over R can be expressed uniquely as

$$C=C_1+uC_2.$$

In order to describe the property of the skew reciprocal polynomial we need the following morphism of rings [19]:

$$\ominus:\Re\to\Re$$
$$\ominus(\sum_{i=0}^{t}a_ix^i)=\sum_{i=0}^{t}\Theta(a_i)x^i$$

Definition 3: ([10, Definition 2]) Let R be a commutative finite ring. The skew reciprocal polynomial of degree m

$$h=\sum_{i=0}^{m}h_iX^i\in\Re$$

is

$$h^*=\sum_{i=0}^{m}X^{m-i}.h_i=\sum_{i=0}^{m}\Theta^i\left(h_{m-i}\right)X^i.$$

The left monic skew reciprocal polynomial of h is $h^{\natural}=\frac{1}{\Theta^m(h_0)}h^*$. The skew polynomial h is self-reciprocal if $h=h^{\natural}$.

Lemma 2: Let $f\in\Re$ be a skew polynomial of degree n such that $f=hg$, where h and g are skew polynomials of degrees k and $n-k$. Then

1) $f^*=\ominus^k(g^*)h^*$
2) $(f^*)^*=\ominus^n(f)$

Proof. Let $f=\sum_{i=0}^{n}f_ix^i, g=\sum_{i=0}^{r}f_ix^i$ and $h=\sum_{i=0}^{k}h_ix^i\in\Re$ be skew polynomials of degrees n,r,k with $n=k+r$.

1) For $l\in\{0,\ldots,n\}$, the $l-$th coefficient of f is

$$f_l=\sum_{\substack{i+j=l\\0\le i\le k\\0\le j\le r}}h_i\Theta^i(g_i).$$

By Definition 3, we have $f_l^* = \Theta^l(f_{n-l})$ then, the $l-$th coefficient of f^* defined by

$$\begin{aligned} f_l^* &= \sum_{\substack{i+j=n-l \\ 0\le i\le k \\ 0\le j\le r}} \Theta^l(h_i)\Theta^{l+i}(g_j) \\ &= \sum_{\substack{k-i+r-j=n-l \\ 0\le i\le k \\ 0\le j\le r}} \Theta^l(h_{k-i})\Theta^{l+k-i}(g_{r-j}) \\ &= \sum_{\substack{i+j=l \\ 0\le i\le k \\ 0\le j\le r}} \Theta^j(\Theta^i(h_{k-i}))\Theta^k(\Theta^j(g_{r-j})) \\ &= \sum_{\substack{i+j=l \\ 0\le i\le k \\ 0\le j\le r}} \Theta^k(g_j^*)\Theta^j(h_i^*), \end{aligned}$$

and this implies that $f^* = \ominus^k(g^*)h^*$.

2) $(f^*)^* = \sum_{i=0}^n \Theta^i(f_{n-i}^*)x^i = \sum_{i=0}^n \Theta^i(\Theta^{n-i}(f_i))x^i = \ominus^n(f)$.

■

III. Skew Cyclic and Skew Negacyclic Codes over R

If $f(x) \in R[x,\Theta]$, we use the notation $\langle f(x)\rangle$ for the left ideal generated by $f(x)$. To study constacyclic codes over R, we first consider some structural properties of $R[x,\Theta]/\langle x^n - \lambda\rangle$.

In the following, we generalize the structure and properties from [28] to codes over $\mathbb{Z}_q + u\mathbb{Z}_q$.

Definition 4: [28, Definition 2] Let C be a skew cyclic (resp. skew negacyclic) code over R of length n and let $f(x)$ be a polynomial in C of minimal degree. If $f(x)$ is a monic polynomial, then $C = \langle f(x)\rangle$, where $f(x)$ is a right divisor of $x^n - 1$ (resp. $x^n + 1$).

Theorem 3.1: The ring $R[x,\Theta]/\langle x^n - 1\rangle$ (resp. $R[x,\Theta]/\langle x^n + 1\rangle$) is not a principal ideal ring.

Proof. The proof is similar to the proof of [4, Theorem 9]. ■

Therefore, a skew cyclic (resp. skew negacyclic) code of length n over R is in general not principally generated. However, the ring $\frac{\mathbb{Z}_q[x,\theta]}{\langle x^n-1\rangle}$ $\left(\text{ resp. } \frac{\mathbb{Z}_q[x,\theta]}{\langle x^n+1\rangle}\right)$ is a principal ideal ring. Therefore a skew cyclic (resp. skew negacyclic) code of length n over R is of the form $C = C_1 + uC_2 = g_1 + ug_2$, where $g_1, g_2 \in \mathbb{Z}_q$ are generator polynomials of the skew cyclic (resp. skew negacyclic) codes C_1, C_2, respectively.

Theorem 3.2: Let C be a skew linear code over R of length n and $C = C_1 + uC_2$ be its decomposition, where C_1 and C_2 are codes over $\mathbb{Z}_q$ of length n. If C is a skew constacyclic code with respect to the automorphism Θ, then C_1 and C_2 are skew constacyclic codes over $\mathbb{Z}_q$ with respect to the automorphism θ.

Proof. Let $\rho_{\Theta,\lambda}$ be the skew constacyclic shift operator on R^n, and Let $\rho_{\theta,\lambda}$ be the skew constacyclic shift operator on $\mathbb{Z}_q^n$, For any $c \in C$, we have $\rho_{\Theta,\lambda}(c) = \rho_{\Theta,\lambda}(c_1) + u\rho_{\Theta,\lambda}(c_2)$, where $c = c_1 + uc_2$. Assume that C_1, C_2 are skew constacyclic codes over $\mathbb{Z}_q$. Then, we have that $\rho_{\theta,\lambda}(c_1) \in C_1$ and $\rho_{\theta,\lambda}(c_2) \in C_2$, furthermore, $\rho_{\Theta,\lambda}(c_1) \in C_1$ and $\rho_{\Theta,\lambda}(c_2) \in C_2$ (because $\Theta(c_i) = \theta(c_i)$ for all $c_i \in \mathbb{Z}_q$). So $\rho_{\Theta,\lambda} \in C$. Which implies that C is skew constacyclic code.

Conversely, suppose that C is a skew constacyclic code of length n over R, then $\rho_{\Theta,\lambda}(c) \in C$, This implies that $\rho_{\Theta,\lambda}(c_1) + u\rho_{\Theta,\lambda}(c_2) \in C$ and since $\Theta(a) = \theta(a)$ for all $a \in \mathbb{Z}_q$, we have $\rho_{\Theta,\lambda}(c_1) = \rho_{\theta,\lambda}(c_1)$ and $\rho_{\Theta,\lambda}(c_2) = \rho_{\theta,\lambda}(c_2)$, so we have $\rho_{\theta,\lambda}(c_1) + u\rho_{\theta,\lambda}(c_2) \in C$. Then, by the definition of C_1 and $C_2, \rho_{\theta,\lambda}(c_1) \in C_1$ and $\rho_{\theta,\lambda}(c_2) \in C_2$. Thus, C_1 and C_2 are skew constacyclic codes over $\mathbb{Z}_q$. ■

Corollary 1: Let C be a skew linear code over R of length n and $C = C_1 + uC_2$ be its decomposition, where C_1 and C_2 are codes over $\mathbb{Z}_q$ of length n. Then C is a skew cyclic (resp. skew negacyclic) code with respect to the automorphism Θ if and only if C_1 and C_2 are skew cyclic (resp. skew negacyclic) codes over $\mathbb{Z}_q$ with respect to the automorphism θ.

In the next, we will give a formula for the number of skew cyclic (resp. skew negacyclic) codes of length n over $R = \mathbb{Z}_q + u\mathbb{Z}_q$. Before that we need to give the following Remark.

Remark 1: According to the preliminaries section, we have for all $a \in \mathbb{Z}_q$, $\theta(a) = a$. Which means that $\mathbb{Z}_q$ is the fixed subring under θ. Therefore, for any monic right divisor $g(x) \in \mathbb{Z}_q[x,\theta]$ of $x^n - \epsilon$, with $\epsilon \in \{-1, 1\}$, we have $g(x) \in \mathbb{Z}_q[x]$. Therefore, monic irreducible factors of $x^n - \epsilon$ with $\epsilon \in \{-1, 1\}$ in $\mathbb{Z}_q[x,\theta]$, are same as the irreducible factors of $x^n - \epsilon$ in the polynomial ring $\mathbb{Z}_q[x]$.

We use the precedent remark for giving the following Theorem.

Theorem 3.3: Let $x^n - \epsilon = \prod_{l=1}^b \pi_i^l(x), i \in \mathbb{N}$ where $\epsilon \in \{-1, 1\}$ and $\pi_i(x) \in \mathbb{Z}_q[x,\theta]$ is irreducible. Then the number of skew cyclic (resp. skew negacyclic) codes of length n over $R = \mathbb{Z}_q + u\mathbb{Z}_q$ is equal to $(i+1)^{2b}$.

Proof. It follow from Remark 1 that $\pi_i(x) \in \mathbb{Z}_q[x]$. In this case the number of skew cyclic (resp. skew negacyclic) codes of length n over $\mathbb{Z}_q$ is $(i+1)^b$ (because from [17, Corollary 4.12] we have that the number of cyclic and negacyclic codes over $\mathbb{Z}_q$ is equal to $(i+1)^b$.) Hence by the decomposition theorem, $(i+1)^{2b}$ is the number of skew cyclic (resp. skew negacyclic) codes of length n over $R = \mathbb{Z}_q + u\mathbb{Z}_q$. ■

In the next, we determine a necessary condition and a sufficient condition for the skew cyclic (resp. skew negacyclic) codes over R to be free. Before that, according to [28] we have the following theorems.

Theorem 3.4: [28, Theorem 4] If C is a skew cyclic (resp. skew negacyclic) code of length n over R containing a minimum degree polynomial $g(x)$ whose leading coefficient is a unit, then C is a free code such that $C = \langle g(x)\rangle$ and $g(x) \mid x^n - 1$.(resp. $g(x) \mid x^n + 1$). Moreover, C has a basis $\{g(x), xg(x), \ldots, x^{n-deg(g(x))-1}\}$ and $|C| = |R|^{n-deg(g(x))}$.

Theorem 3.5: [28, Theorem 5] Let C is a free principally generated skew cyclic (resp. skew negacyclic) code of length n over R. Then there exists a minimal degree polynomial $g(x) \in C$ having its leading coefficient a unit such that $C = \langle g(x)\rangle$ and $g(x) \mid x^n - 1$.(resp. $g(x) \mid x^n + 1$).

The following result gives a sufficient condition for a skew cyclic (resp. skew negacyclic) code C over R to be a free

$\mathbb{Z}_q-$code.

Theorem 3.6: Let $C = C_1 + uC_2$ be a skew cyclic (resp. skew negacyclic) code of length n over R. If C_1, C_2 are free code over $\mathbb{Z}_q$, then C is a free $\mathbb{Z}_q-$module.

Proof. Assume that C_1, C_2 are $\mathbb{Z}_q-$free code of ranks k_1, k_2, respectively. Let $\{c_{11}, c_{12}, \ldots, c_{1k_1}\}$ and $\{c_{21}, c_{22}, \ldots, c_{2k_2}\}$ be $\mathbb{Z}_q-$bases of C_1, C_2, respectively. Then the set $\{c_{11}, c_{12}, \ldots, c_{1k_1}, uc_{21}, uc_{22}, \ldots, uc_{2k_2}\}$ spans C, as every element of C can be expressed as a linear combination of elements of this set. Now suppose there exist scalars $a_i, b_j \in \mathbb{Z}_q$ such that $\sum_{i=1}^{k_1} a_i c_{1i} + u\sum_{j=1}^{k_2} b_j c_{2j} = 0$. Then $\sum_{i=1}^{k_1} a_i c_{1i} = 0$ and $u\sum_{j=1}^{k_2} b_j c_{2j} = 0$. Since the elements $c_{11}, c_{12}, \ldots, c_{1k_1}$ are independent and so are the elements $c_{21}, c_{22}, \ldots, c_{2k_2}$, therefore, for all i and j, $a_i = 0$ and $b_j = 0$. Hence C is a $\mathbb{Z}_q-$free module. ■

Theorem 3.7: If $C = C_1 + uC_2$ be a free skew cyclic (resp. skew negacyclic) code of length n over R, then so is C_1 over $\mathbb{Z}_q$.

Proof. Following theorem 3.5, if C is a free skew cyclic (resp. skew negacyclic) code over R with generator polynomial $g(x)$ then $x^n - \epsilon = g(x)h(x)$, with $\epsilon \in \{-1, 1\}$. We can express $g(x) = g_1(x) + ug_2(x)$ and $h(x) = h_1(x) + uh_2(x)$, where $g_1(x), g_2(x), h_1(x), h_2(x) \in \mathbb{Z}_q[x, \theta]$. Then $x^n - \epsilon = g_1(x)h_1(x)(mod\ u)$. The result follows. ■

In the following Proposition, we focus the relationship between skew negacyclic, negacyclic codes and quasi-negacyclic codes over R.

Proposition 2: Let C be a skew negacyclic code of length n and let Θ be an automorphism of R with order e. If $gcd(e, n) = 1$ then C is a negacyclic code of length n over R.

Proof. Let C be a skew negacyclic code of length n such that $\gcd(e, n) = 1$. We know that there exist integers α_1, α_2 such that $\alpha_1 e + \alpha_2 n = 1$. Thus $\alpha_1 e = 1 - \alpha_2 n$. We may assume that α_2 is a negative integer, so we can write $\alpha_1 e = 1 + ln$ where $l > 0$. Let $c(x) = c_0 + c_1 x + \cdots + c_{n-1}x^{n-1}$ be a codeword in C.

To show that C is a negacyclic code it is suffices to show that $-c_{n-1}x^{n-1} + c_0 + c_1 x + \cdots + c_{n-2}x^{n-2} \in C$. Note that for $x^{\alpha_1 e}c(x) = \Theta^{\alpha_1 e}(c_0)x^{1+ln} + \Theta^{\alpha_1 e}(c_1)x^{2+ln} + \cdots + \Theta^{\alpha_1 e}(c_{n-1})x^{n+ln} \in C$, Note that in the ring $\Re/\langle x^n + 1\rangle$, we have $x^n = -1$ and for any $\alpha_1 \in R$ and $\Theta^e(\alpha_1) = \alpha_1$. This implies that

$$x^{\alpha_1 e}C(x) = -c_{n-1} + c_0 x + \cdots + c_{n-2}x^{n-2} \in C.$$

Thus, C is a negacyclic code of length n. ■

Definition 5: Let $n = s\ell$. skew quasi negacyclic code C over R of length n and index ℓ is a linear code with the property that if

$$c = \begin{pmatrix} c_{0,0}, c_{0,1}, \ldots, c_{0,\ell-1}, c_{1,0}, c_{1,1}, \ldots, c_{1,\ell-1}, \ldots, \\ c_{s-1,0}, c_{s-1,1}, \ldots, c_{s-1,\ell-1} \end{pmatrix} \in C,$$

then

$$\tau_{\Theta,\ell}(c) = \begin{pmatrix} -\Theta(c_{s-1,0}), \ldots, -\Theta(c_{s-1,\ell-1}), \\ \Theta(c_{0,0}), \ldots, \Theta(c_{0,\ell-1}), \ldots, \\ \Theta(c_{s-2,0}), \ldots, \Theta(c_{s-2,\ell-1}) \end{pmatrix} \in C,$$

where $\tau_{\Theta,\ell}$ is a skew quasi-negacyclic shift operator and ℓ is the smallest positive integer satisfying this condition. Further, if Θ is the identity map, He become the classical quasi-negacyclic and we denote τ_ℓ is a quasi-negacyclic shift operator.

Proposition 3: Let C be a skew negacyclic code of length n over R and let Θ be an automorphism with order e. If $gcd(e, n) = \ell$, then C is equivalent to a quasi-negacyclic code of length n with index ℓ.

Proof. Let $n = s\ell$ and

$$\begin{pmatrix} c_{0,0}, c_{0,1}, \ldots, c_{0,\ell-1}, c_{1,0}, c_{1,1}, \ldots, c_{1,\ell-1}, \ldots, \\ c_{s-1,0}, c_{s-1,1}, \ldots, c_{s-1,\ell-1} \end{pmatrix} \in C.$$

Since $gcd(e, n) = \ell$, there exists integers a_1, a_2 such that $a_1 e + a_2 n = \ell$.

Therefore $a_1 e = \ell - a_2 n = \ell + jn$, where j is a nonnegative integer. Consider

$$\Theta^{a_1 e}\begin{pmatrix} c_{0,0}, c_{0,1}, \ldots, c_{0,\ell-1}, c_{1,0}, c_{1,1}, \ldots, c_{1,\ell-1}, \ldots, \\ c_{s-1,0}, c_{s-1,1}, \ldots, c_{s-1,\ell-1} \end{pmatrix}$$
$$= \begin{pmatrix} -\Theta^{\ell+jn}(c_{s-1,0}), \ldots, -\Theta^{\ell+jn}(c_{s-1,\ell-1}), \\ \Theta^{\ell+jn}(c_{0,0}), \ldots, \Theta^{\ell+jn}(c_{0,\ell-1}), \\ \ldots, \\ \Theta^{\ell+jn}(c_{s-2,0}), \ldots, \Theta^{\ell+jn}(c_{s-2,\ell-1}) \end{pmatrix}.$$

Since the order of Θ is e, $\Theta^{\ell+jn}(a) = \Theta^{a_1 e}(a) = a$ for any $a \in R$ which implies that

$$\Theta^{a_1 e}\begin{pmatrix} c_{0,0}, c_{0,1}, \ldots, c_{0,\ell-1}, c_{1,0}, c_{1,1}, \ldots, c_{1,\ell-1}, \ldots, \\ c_{s-1,0}, c_{s-1,1}, \ldots, c_{s-1,\ell-1} \end{pmatrix}$$
$$= \begin{pmatrix} -c_{s-1,0}, -c_{s-1,1}, \ldots, -c_{s-1,\ell-1}, c_{0,0}, \ldots, \\ c_{0,\ell-1}, \ldots, c_{s-2,0}, c_{s-2,1}, \ldots, c_{s-2,\ell-1} \end{pmatrix} \in C.$$

Thus, C is a quasi-negacyclic code of length n with index ℓ over R. ■

IV. Gray Images of Skew Negayclic and Skew Cyclic Codes Over R

In this section, we give a characterization of the Gray images of skew cyclic (resp. skew negacyclic) codes over R. We know that every element of R can be expressed as $a + ub$, where $a, b \in \mathbb{Z}_q$. According to Sharama $et al.$ [27] we have the following Gray map

$$\Phi\colon R^n \to \mathbb{Z}_q^{2n}$$
$$\Phi(a + ub) = (b, a + b), \tag{4}$$

where $a, b \in \mathbb{Z}_q^n$. Following [2] and [31], the Lee weight is defined as the Hamming weight of the Gray image

$$w_L(a+ub) = w_H(b) + w_H(a+b), \text{ for } a, b \in \mathbb{Z}_q^n.$$

The Lee distance of $x, y \in R^n$ is defined as $w_L(x-y)$. Furthermore, according to [2, Proposition 3.1], the Gray map Φ is a linear distance preserving map from (R^n, Lee distance) to ($\mathbb{Z}_q^{2n}$, Hamming distance). Moreover, it is an isometry from R^n to $\mathbb{Z}_q^{2n}$.

A. Gray Image of Skew Negacyclic codes

Let $\sigma : \mathbb{Z}_q^{2n} \to \mathbb{Z}_q^{2n}$ be a skew quasi negacyclic shift operator defined by

$$\sigma(a^{(1)} \mid a^{(2)}) = (\rho_{\theta,-1}(a^{(1)}) \mid \rho_{\theta,-1}(a^{(2)})),$$

where $a^{(1)}, a^{(2)} \in \mathbb{Z}_q^n, \mid$ a vector concatenation and $\rho_{\theta,-1}$ is a skew negacyclic shift operator as define in the precedent section. A skew linear code C of length $2n$ over $\mathbb{Z}_q$ is said to be skew quasi negacyclic code of index 2 if $\sigma(C) = C$.

In addition, for each $\Theta \in$ Aut(R), let $T_\Theta : R^n \mapsto R^n$ be a linear transformation given by

$$T_\Theta(a_0, a_1 \ldots, a_{\beta-1}) = (\Theta(a_0), \Theta(a_1) \ldots, \Theta(a_{\beta-1})).$$

Remark 2: C is a skew negacyclic code if and only if $T_\Theta \circ \rho_{-1}(C) = C$.

Proposition 4: Under the previous notation we have:

$$T_\Theta \circ \Phi \circ \rho_{-1} = \sigma \circ \Phi$$

Proof. Let $r = (r_0, r_1, \ldots, r_{n-1}) \in R^n$, where $r_i = a_i + ub_i$, then we can write $\Phi(r) = (b_i, a_i + ub_i)$. Then we have:

$$\Phi(\rho_{-1}(r)) = (-b_{n-1}, b_0, \ldots, b_{n-2}, -(a_{n-1} + b_{n-1}), a_0 + b_0, \ldots, a_{n-2} + b_{n-2}).$$

Now we apply T_Θ in the above equation we get,

$$\begin{aligned} T_\Theta \circ \Phi(\rho_{-1}(r)) &= T_\Theta(-b_{n-1}, b_0, \ldots, b_{n-2}, -(a_{n-1} \\ &\quad +b_{n-1}), a_0 + b_0, \ldots, a_{n-2} + b_{n-2}) \\ &= \begin{pmatrix} \Theta(-b_{n-1}), \Theta(b_0), \ldots, \Theta(b_{n-2}), -\Theta(a_{n-1} \\ +b_{n-1}), \Theta(a_0 + b_0), \ldots, \Theta(a_{n-2} + b_{n-2}) \end{pmatrix}, \end{aligned}$$

since, for any $a \in \mathbb{Z}_q$, $\Theta(a) = \theta(a)$ where $\theta \in \mathbb{Z}_q$. So, we have

$$T_\Theta \circ \Phi \circ \rho_{-1}(r) = \begin{pmatrix} -\theta(b_{n-1}), \theta(b_0), \ldots, \theta(b_{n-2}), -\theta(a_{n-1} + b_{n-1}), \\ \theta(a_0 + b_0), \ldots, \theta(a_{n-2} + b_{n-2}), \end{pmatrix}$$

On the other hand, $\sigma(\Phi(r)) = \sigma(b_0, b_1, \ldots, b_{n-1}, a_0 + b_0, a_1 + b_1, \ldots, a_{n-1} + b_{n-1})$

$$= \begin{pmatrix} -\theta(b_{n-1}), \theta(b_0), \ldots, \theta(b_{n-2}), -\theta(a_{n-1} + b_{n-1}), \\ \theta(a_0 + b_0), \ldots, \theta(a_{n-2} + b_{n-2}). \end{pmatrix}$$

On the other hand, $\sigma(\Phi(r)) = \sigma(b_0, b_1, \ldots, b_{n-1}, a_0 + b_0, a_1 + b_1, \ldots, a_{n-1} + b_{n-1})$

$$= \begin{pmatrix} -\theta(b_{n-1}), \theta(b_0), \ldots, \theta(b_{n-2}), -\theta(a_{n-1} + b_{n-1}), \\ \theta(a_0 + b_0), \ldots, \theta(a_{n-2} + b_{n-2}). \end{pmatrix}$$

Then the result follows. ■

Theorem 4.1: Let C be a code of length n over R and Θ is an automorphism of R. Then C is a skew negacyclic code of length n over R if and only if $\Phi(C)$ is a skew quasi negacyclic code of length $2n$ over $\mathbb{Z}_q$ of index 2.

Proof. Assume that C is skew negacyclic code. Then $T_\Theta \circ \rho_{-1}(C) = C$. Now we may assume that C is negacyclic code then, we have that $\rho_{-1}(C) = C$, if we apply Φ and then we apply T_Θ we get

$$T_\Theta(\Phi(\rho_{-1}(C))) = T_\Theta(\Phi(C)) = \Phi(C),$$

where C is a skew negacyclic code and from Proposition 4,

$$\sigma(\Phi(C)) = T_\Theta(\Phi(\rho_{-1}(C))) = \Phi(C).$$

Hence $\Phi(C)$ is a skew quasi negacyclic code of index 2. Conversely, if $\Phi(C)$ is a skew quasi negacyclic code of index 2, then

$$\sigma(\Phi(C)) = \Phi(C).$$

From Proposition 4, we have

$$\Phi(C) = \sigma(\Phi(C)) = T_\Theta(\Phi(\rho_{-1}(C))).$$

Since Φ is injective, it follows that $T_\Theta(\rho_{\Theta,-1})(C) = C$. ■

B. Gray image of Skew Cyclic codes over R of odd length

In this subsection, we give a characterization of the Gray images of skew cyclic codes of odd length n over R with even characteristic.

Theorem 4.2: [28, Theorem 3] A code C of length n in $R_n = \Re/\langle x^n - 1\rangle$(resp. $\Re/\langle x^n + 1\rangle$) is a skew cyclic (resp. skew negacyclic) code if and only if C is a left $\Re-$submodule of the left $\Re-$module R_n.

Proposition 5: Let $\upsilon : \Re/\langle x^n - 1\rangle \to \Re/\langle x^n + 1\rangle$ be defined as :

$$\upsilon(c(x)) = c(-x).$$

If n is odd, then υ is a left $R-$module isomorphism.

Proof. Justification is straightforward. Only need to observe that if

$$\begin{aligned} &a(x) \equiv b(x) \bmod (x^n - 1) \\ \Leftrightarrow\ &a(x) - b(x) = d(x)(x^n - 1) \text{ for some } d(x) \in R[x, \Theta] \\ \Leftrightarrow\ &a(-x) - b(-x) = d(-x)((-1)^n x^n - 1) \\ =\ &d(-x)(-x^n - 1)(\text{ as } (-1)^n = -1 \text{ if } n \text{ is odd}) \\ =\ &(-1)d(-x)(x^n + 1) \\ \Leftrightarrow\ &a(-x) \equiv b(-x) \bmod (x^n + 1) \end{aligned}$$

■

As an immediate consequence, we obtain:

Corollary 2: I is an ideal of $R[x, \Theta]/\langle x^n - 1\rangle$ if and only if $\upsilon(I)$ is an ideal of $R[x, \Theta]/\langle x^n + 1\rangle$.

Corollary 3: Let μ be the permutation of R^n with n odd, such that $\mu(c_0, c_1, \ldots, c_{n-1}) = (c_0, (-1)c_1, \ldots, (-1)^{n-1}c_{n-1})$, and C be a non-empty subset of R^n. Then C is a skew cyclic code of length n if and only if $\mu(C)$ is a skew negacyclic codes of length n over R.

Now define two maps a and b of R into $\mathbb{Z}q$ such that, if $\lambda \in R$ then the $p-$adic expansion of λ is $\lambda = a(\lambda) + ub(\lambda)$. We remark the following obvious property

$$a(-\lambda) = a(\lambda), b(-\lambda) = a(\lambda) + b(\lambda) \tag{5}$$

We introduce the following permutation of $\mathbb{Z}_q^{2n}$ from [30] which is called the Nechaev permutation.

Definition 6: Let n be an odd integer and ψ be the permutation of $\{0, 1, 2, \ldots, 2n-1\}$ given by

$$\psi = (1, n+1)(3, n+3)\ldots(2i+1, n+2i+1)\ldots(n-2, 2n-2).$$

The Nechaev permutation is the permutation ϱ of $\mathbb{Z}_q^{2n}$ defined by

$$\varrho(r_0, r_1, \ldots, r_{2n-1}) = (r_{\psi(0)}, r_{\psi(1)}, \ldots, r_{\psi(2n-1)}).$$

Proposition 6: $\Phi \circ \mu = \varrho \circ \Phi$.

Proof. Let $(r_0, r_1, \ldots, r_{n-1}) \in R^n$ where $r_i = a_i + ub_i, 0 \leq i \leq n-1$. From

$$\mu(r) = (r_0, (-1)r_1, \ldots, (-1)^{n-1}r_{n-1}),$$

and from (5). It follow that

$$(\Phi\mu)(r) = (b_0, a_1 + b_1, b_2, \ldots, a_{n-2} + b_{n-2}, b_{n-1}, a_0 + b_0, b_1, a_2 + b_2, \ldots, b_{n-2}, a_{n-1} + b_{n-1}).$$

On the other hand, since
$\Phi(r) = (b_0, b_1, \ldots, b_{n-1}, a_0 + b_0, a_1 + b_1, \ldots, a_{n-1} + b_{n-1})$,
$(\varrho\Phi)(r) = \varrho(b_0, b_1, \ldots, b_{n-1}, a_0 + b_0, a_1 + b_1, \ldots, a_{n-1} + b_{n-1})$
$= (b_0, a_1 + b_1, b_2, \ldots, a_{n-2} + b_{n-2}, b_{n-1}, a_0 + b_0, b_1, a_2 + b_2, \ldots, b_{n-2}, a_{n-1} + b_{n-1})$. Therefore $(\Phi\mu)(r) = (\varrho\Phi)(r)$ and so $\Phi\mu = \varrho\Phi$. ■

Corollary 4: The Gray image of a skew cyclic code of odd length n over R is equivalent to a skew quasi-negacyclic code of length $2n$ over $\mathbb{Z}_q$ of index 2.

Proof. From Corollary 3, a code C of odd length n over R is skew cyclic if and only if $\mu(C)$ is a skew negacyclic code. By Theorem 4.1, this is true if and only if $\Phi(\mu(C))$ is a skew quasi-negacyclic code of index 2 over $\mathbb{Z}_q$, i.e. if and only if $\varrho(\Phi(C))$ is a skew quasi-negacyclic code of index 2 over $\mathbb{Z}_q$. ■

V. Self-Orthogonal Skew Cyclic and Skew negacyclic Codes Over R

In this section, we give a necessary and sufficient condition for skew cyclic (resp. skew negacyclic) codes over $\mathbb{Z}_q + u\mathbb{Z}_q$ that contain its dual. We first require some theorems.

Proposition 7: Let $C = C_1 + uC_2$ be a skew cyclic (resp. skew negacyclic) code of length n over R. Then $C = \langle g_1, ug_2\rangle$ and $|C| = q^{2n-(deg(g_1(x))+deg(g_2(x)))}$, where g_1, g_2 are the generator polynomials of C_1 and C_2, respectively.

Proof. Assume that$C = C_1 + uC_2$ be a skew cyclic (resp. skew negacyclic) codes so C_1 and C_2 are skew cyclic (resp. skew negacyclic) codes over $\mathbb{Z}_q$, which implies that $C_i = (g_i) \subseteq \mathbb{Z}_q[x, \theta]/(x^n - \epsilon)$ with $i = 1, 2$ and $\epsilon \in \{-1, 1\}$. Also, since $C = C_1 + uC_2$ we can write C as $C = \{g(x); g(x) = g_1(x) + ug_2(x)\}$ where $g_1(x) \in C_1$ and $g_2(x) \in C_2$, thus $C \subseteq \langle g_1, ug_2\rangle \subseteq R[x, \Theta]/(x^n - \epsilon)$ with $\epsilon \in \{-1, 1\}$.
On the other hand, let $g_1(x)f_1(x) + ug_2(x)f_2(x) \in \langle g_1(x), ug_2(x)\rangle$, where f_1 and f_2 are the elements of $\Re/(x^n - \epsilon)$ with $\epsilon \in \{-1, 1\}$. Then there exists $r_1(x), r_2(x) \in \mathbb{Z}_q[x, \theta]/(x^n - \epsilon)$ such that $f_1(x) = r_1(x)$ and $uf_2(x) = ur_2(x)$. Therefore, $\langle g_1, ug_2\rangle \subseteq C$. Thus, $C = \langle g_1, ug_2\rangle$.
■

Proposition 8: Let C be a skew cyclic (resp. skew negacyclic) code over R, then there is unique skew polynomial $g(x)$ such that $C = \langle g(x)\rangle$ and $g(x) \mid (x^n - 1), (\text{ resp } g(x) \mid (x^n + 1))$ and $g(x) = g_1(x) + ug_2(x)$, where $g_0(x), g_1(x) \in \mathbb{Z}_q[x, \theta]$.

Proof. We know that C is a left ideal of $\Re/(x^n - 1), (\text{ resp } \Re/(x^n+1))$. According to [28], we have that C generated by a monic skew polynomial $g(x)$ such that $g(x) \mid x^n - 1(\text{ resp } g(x) \mid (x^n + 1))$. Furthermore, from Theorem 4.1 (i) and Proposition 4.1 of [20], $C = \langle g(x)\rangle = \langle g_1(x) + ug_2(x)\rangle$, where $g(x)$ is unique and $g_1(x), g_2(x) \in \mathbb{Z}_q[x, \theta]$.
■

Proposition 9: Let C be a skew linear code of length n over R, then $C^\perp = C_1^\perp + uC_2^\perp$. Moreover,

(i) if C is a skew cyclic (resp. skew negacyclic) code of length n over R, then $C^\perp$ is also a skew cyclic (resp. skew negacyclic) code of length n over R.
(ii) C is self-dual skew cyclic (resp. self-dual skew negacyclic) if and only if C_1 and C_2 are self-dual skew skew cyclic (resp. self-dual skew negacyclic) of length n over $\mathbb{Z}_q$.

Proof. Define $\hat{C}_1 = \{x \in \mathbb{Z}_q^n \mid \exists y \in \mathbb{Z}_q^n, x + uy \in C^\perp\}$ and $\hat{C}_2 = \{y \in \mathbb{Z}_q^n \mid \exists x \in \mathbb{Z}_q^n, x + uy \in C^\perp\}$. Then $C^\perp = \hat{C}_1 + u\hat{C}_2$ and this expression is unique. Clearly, $\hat{C}_1 \subseteq C_1^\perp$. Let c_1 be an element of $C_1^\perp$. Then, for any $x \in C_1$, there exists $y \in \mathbb{Z}_q^n$ such that: if $x = a + ub \in C$ and $y = c + ud \in C^\perp$, then x.y=0 gives $a.c = 0, bc = 0$ and $a.d = 0$. Then $\hat{C}_1 \subset C_1^\perp$, as for any $c \in \hat{C}_1, a.c = 0$ for all $a \in C_1$. In reverse direction, let $c_1 \in C_1^\perp$ and $x = a + ub \in C$, then $uc_1.x = 0$, and so, $uc_1 \in C^\perp$. By the unique expression of $C^\perp$, we have $c_1 \in \hat{C}_1$, so $\hat{C}_1 = C_1^\perp$. Similarly, we can prove $\hat{C}_2 = C_2^\perp$ implying $C^\perp = C_1^\perp + uC_2^\perp$.

(i) Let C be a skew cyclic (resp. skew negacyclic) code over R. Then from Corollary 1, C_1 and C_2 are skew cyclic (resp. skew negacyclic) codes over $\mathbb{Z}_q$, since the dual of skew cyclic (resp. skew negacyclic) code over $\mathbb{Z}_q$ is a skew cyclic (resp. skew negacyclic) code. Again from Corollary 1 and the above discussion, $C^\perp$ is a skew cyclic (resp. skew negacyclic)code over R.
(ii) Clearly, if C is self-dual skew cyclic (resp. skew negacyclic) codes over R, then C_1 and C_2 are self-orthogonal over $\mathbb{Z}_q$. i.e: $C_1 \subseteq C_1^\perp$ and $C_2 \subseteq C_2^\perp$, let $c_1 \in C_1^\perp$. Then there exists $l \in \mathbb{Z}_q$ such that $c_1 + ul \in C^\perp = C$.

by unique expression of elements of C, $c \in C_1$ and so $C_1^{\perp} = C_1$. Similarly, $C_2^{\perp} = C_2$. Hence the result. Conversely, assume that C_1 and C_2 are self-dual skew cyclic (resp. skew negacyclic) codes over $\mathbb{Z}_q$. Then C is a self-dual skew cyclic (resp. skew negacyclic) codes over R as $C^{\perp} = C_1^{\perp} + uC_2^{\perp}$. ■

Definition 7: [27, Theorem 9] Let C be a skew cyclic (resp. skew negacyclic) code of even length n generated by a minimum degree monic polynomial $g(x) = g_0 + g_1x + \cdots + g_{n-k}x^{n-k-1} + x^{n-k}$ such that $x^n - \epsilon = h(x)g(x)$ with $\epsilon \in \{-1, 1\}$ for some $h(x) \in \Re/(x^n - \epsilon)$. Let $h(x) = h_0 + h_1x + \cdots + h_{k-1}x^{k-1} + x^{k-1} + x^k$. Then the skew polynomial $h^*(x) = 1 + \Theta(h_{k-1})x + \cdots + \Theta^k(h_0)x^k$. generates $C^{\perp}$.

Proposition 10: Let C_1, C_2 be a skew cyclic (resp. skew negacyclic) code over $\mathbb{Z}_q$ with generator polynomials g_1, g_2 such that $x^n - 1 = h_1(x)g_1(x)$ and $x^n - 1 = h_2(x)g_2(x)$ (resp. $x^n + 1 = h_1(x)g_1(x)$ and $x^n + 1 = h_2(x)g_2(x)$) in $\mathbb{Z}_q[x, \theta]$. If $C = C_1 + uC_2$, then

$$C^{\perp} = \langle h_1^{\natural}(x) + uh_2^{\natural}(x) \rangle$$

and $|C^{\perp}| = q^{(deg(g_1)+deg(g_2))}$ where $h_1^{\natural}$ and $h_2^{\natural}$ are the left monic skew reciprocal polynomials of h_1, h_2 respectively.

Proof. Following from Definition 7, $C^{\perp} = \langle h^*(x) \rangle$, where h^* is the skew reciprocal polynomial of h, and from [11], we have that the $C^{\perp} = \langle h^{\natural}(x) \rangle$ where h satisfies simultaneously $\ominus^n(h)g = x^n - \epsilon$ and $gh = x^n - \Theta^{-k}(\epsilon)$ with $\epsilon \in \{-1, 1\}$. Furthermore, according to Proposition 9, we know that $C^{\perp} = C_1^{\perp} + uC_2^{\perp}$. Therefore, since $C_1^{\perp} = \langle h_1^{\natural}(x) \rangle$ and $C_2^{\perp} = \langle h_2^{\natural}(x) \rangle$, we conclude by Proposition 8 that $C^{\perp} = \langle h_1^{\natural}(x) + uh_2^{\natural}(x) \rangle$. ■

For the rest, we need the following theorem which presents a condition for skew cyclic (resp. skew negacyclic) codes over $\mathbb{Z}_q$ for self-orthogonality.

Theorem 5.1: Let $C = \langle g(x) \rangle$ be a skew cyclic (resp. skew negacyclic) code of length n over $\mathbb{Z}_q$. Then C is a self-orthogonal code if and only if $h^{\natural}$ is a right divisor of $g(x)$.

Proof. Assume that C is a self-orthogonal skew cyclic (resp. skew negacyclic) code of length n over $\mathbb{Z}_q$. Since $g(x) \in C \subset C^{\perp}$, then there exists a polynomial $u(x)$ such that $g(x) = u(x)h^{\natural}(x)$. So the polynomial $h^{\natural}(x)$ is a right divisor of $g(x)$.

Conversely, for any element $c(x) \in C$, there exists a polynomial $v(x)$ such that $c(x) = v(x)g(x)$. Since $g(x)$ is divisible by $h^{\natural}(x)$ on right, we have

$$g(x) = u(x)h^{\natural}(x). \tag{6}$$

Then, we multiply the above equation by $v(x)$, we get

$$\begin{aligned} c(x) = v(x)g(x) &= v(x)[u(x)h^{\natural}(x)] \\ &= [v(x)u(x)]h^{\natural}(x). \end{aligned}$$

Which implies that $c(x) \in C^{\perp}$. So C is self-orthogonal. ■

Theorem 5.2: Let $C = \langle g(x) \rangle$ be a skew cyclic (resp. skew negacyclic) code of even length n over $\mathbb{Z}_q$ such that the order of θ divides n. Then C is a self-orthogonal code if and only if $h^{\natural}(x)h(x)$ is a right divisor of $x^n - 1$(resp. $x^n + 1$).

Proof. Assume that C is a self-orthogonal skew cyclic (resp. skew negacyclic) code of even length n over $\mathbb{Z}_q$. According to Theorem 5.1, we have that $h^{\natural}(x)$ is a right divisor of $g(x)$. So, there exists a polynomial $u(x)$ such that $g(x) = u(x)h^{\natural}(x)$. We multiply both sides of the equation by $h(x)$ on the right, we get:

$$\begin{aligned} x^n - \epsilon = g(x)h(x) &= [u(x)h^{\natural}(x)]h(x) \\ &= u(x)[h^{\natural}(x)h(x)]. \end{aligned}$$

So $h^{\natural}(x)h(x)$ is a right divisor of $x^n - \epsilon$, with $\epsilon\{-1, 1\}$.

Conversely, since $h^{\natural}(x)h(x)$ is a right divisor of $x^n - \epsilon$, we have

$$\begin{aligned} x^n - \epsilon &= v(x)[h^{\natural}(x)h(x)] \\ g(x)h(x) &= v(x)[h^{\natural}(x)h(x)]. \end{aligned}$$

This implies that $(g(x) - v(x)h^{\natural}(x))h(x) = 0$ since $h(x)$ is nonzero polynomial. Therefore, $g(x) - v(x)h^{\natural}(x) = 0$. So we have $g(x) = v(x)h^{\natural}(x)$, and by Theorem 5.1, C is self orthogonal. ■

Corollary 5: Let $C = \langle g(x) \rangle$ be a skew cyclic (resp. skew negacyclic) code of length n over $\mathbb{Z}_q$ such that the order of θ divides n. Then C contains its dual if and only if

$x^n - 1 \equiv 0(mod\ h^{\natural}h)$ (resp. $x^n + 1 \equiv 0(mod\ h^{\natural}h)$).

where $h^{\natural}$ is the left monic skew reciprocal polynomial of h.

Now, we give a necessary and sufficient condition for skew cyclic (resp. skew negacyclic) codes over R to contain its dual.

Theorem 5.3: Let $C = \langle g(x) \rangle = \langle g_1(x) + ug_2(x) \rangle$ be a skew cyclic (resp. skew negacyclic) codes of length n over R such that the order of Θ divides n. Then $C^{\perp} \subseteq C$ if and only if $x^n - 1 \equiv 0(mod\ h_i^{\natural}h_i)$ (resp. $x^n + 1 \equiv 0(mod\ h_i^{\natural}h_i)$) with $i \in \{1, 2\}$.

Proof. Let $x^n - \epsilon \equiv 0(mod\ h_1^{\natural}h_1)$ and $x^n - \epsilon \equiv 0(mod\ h_2^{\natural}h_2)$ with $\epsilon \in \{-1, 1\}$. Then by Corollary 5, we have $C_1^{\perp} \subseteq C_1$ and $C_2^{\perp} \subseteq C_2$. This implies that $C_1^{\perp} \subseteq C_1$ and $uC_2^{\perp} \subseteq uC_2$. Then, $C_1^{\perp} + uC_2^{\perp} \subseteq C_1 + uC_2$. Further,

$$\langle h_1^{\natural}(x) + uh_2^{\natural}(x) \rangle \subseteq \langle g_1(x) + ug_2(x) \rangle.$$

Thus $C^{\perp} \subseteq C$.

Conversely, if $C^{\perp} \subseteq C$ then $C_1^{\perp} + uC_2^{\perp} \subseteq C_1 + uC_2$

$$C^{\perp} = C_1^{\perp} \subseteq C_1 = C$$

$$uC^{\perp} = uC_2^{\perp} \subseteq uC_2 = uC.$$

Thus, $C_1^{\perp} \subseteq C_1$ and $C_2^{\perp} \subseteq C_2$. So, by Corollary 5, $x^n - \epsilon \equiv 0(mod\ h_i^{\natural}h_i)$ with $\epsilon \in \{-1, 1\}$ and $i = 1, 2$. ■

Corollary 6: Let $C = \langle g(x) \rangle$ be a skew cyclic (resp. skew negacyclic) code of length n over R, where $g(x) = g_1(x) + ug_2(x)$, then

$$C^{\perp} \subseteq C \text{ if and only if } C_1^{\perp} \subseteq C_1 \text{ and } C_2^{\perp} \subseteq C_2,$$

where $C_1 = \langle g_1(x) \rangle$ and $C_2 = \langle g_2(x) \rangle$.

REFERENCES

[1] M. C. V. Amarra and F. R. Nemenzo, On $(1-u)-$cyclic codes over $\mathbb{F}_{p^k}+u\mathbb{F}_{p^k}$, Applied Math. Lett., (21), pp. 1129–1133, 2008.

[2] T. Bag and A. K. Upadhyay, Study on negacyclic codes over the ring $\mathbb{Z}_p[u]/\langle u^{k+1}-u\rangle$, J. Appl. Math. Comput, 2018.

[3] R.K. Bandi and M. Bhaintwal, Negacyclic codes over $\mathbb{Z}_4+u\mathbb{Z}_4$, International Journal of Computer Mathematics, 2014.

[4] R.K. Bandi and M. Bhaintwal, Cyclic codes over $\mathbb{Z}_4+u\mathbb{Z}_4$, submited to Adv. Math. Commun., s. Am. Inst. Math. Sci. (AIMS)., 2015.

[5] R.K. Bandi and M. Bhaintwal, A note on cyclic codes over $\mathbb{Z}_4+u\mathbb{Z}_4$, Discrete Mathematics, Algorithms and Applications, (8), 2016.

[6] E-R. Berlekamp, Negacyclic codes for the Lee metric, Proceedings of Conference Combinatorial Mathematics and Its Applications, pp. 298–316. Chapel Hill: Univ, North Carolina Press , 1968.

[7] D. Boucher, W. Geiselmann and F. Ulmer, Skew-cyclic codes, Applicable Algebra in Engineering, Communication and Computing, (18), pp. 379-389, 2007.

[8] D. Boucher and F. Ulmer, Coding with skew polynomial rings, Journal of Symbolic Computation, (44), pp. 1644-1656, 2009.

[9] D. Boucher, P. Sol and F. Ulmer, Skew constacyclic code over Galois rings, Advances in Mathematics of Communications, pp. 273-292, 2008.

[10] D. Boucher and F. Ulmer, A note on the dual codes of module skew codes, Lecture Notes in Computer Science, Cryptography and Coding,7089, pp. 230-243, 2011.

[11] D. Boucher and F. Ulmer, Self-dual skew codes and factorization of skew polynomials, J. Symbolic Comput., 60, pp. 47–61, Jan. 2014.

[12] T. Blackford, Negacyclic codes over $\mathbb{Z}_4$ of even length, IEEE Trans. Inf. Theory, (6), pp. 1417–1424, 2003.

[13] H. Q. Dinh and S. R. Lopez-Permouth, Cyclic and negacyclic codes over finite chain rings, IEEE Trans. Inform. Theory, May, (8), 2004.

[14] J. Gao, F. W. Fu, L. Xiao and R. K. Bandi, Some results on cyclic codes over $\mathbb{Z}_q+u\mathbb{Z}_q$, Discrete Mathematics, Algorithms and Applications, 7 (4), pp. 1–9, 2015.

[15] J. Gao, F. Ma and F. Fu, Skew constacyclic codes over the ring $\mathbb{F}_q+v\mathbb{F}_q$, Appl. Comput. Math., 6(3), pp. 286–295, 2017.

[16] M. Giesbrecht, Factoring in skew-polynomial rings over finite fields, J. Symbolic Comput. 26 (4), pp. 463-486, 1998.

[17] K. Guenda and T–A. Gulliver, MDS and self-dual codes over rings, Finite Fields Appl., (18), pp. 1061–1075, 2012.

[18] F. Gursoy, I. Siap and B. Yildiz, Construction of skew cyclic codes over $\mathbb{F}_p+v\mathbb{F}_p$, Adv. Math. Commun., (8) pp.313–322, 2014.

[19] S. Jitman, S. Ling and P. Udomkavanich, Skew constacyclic codes over Finite Chain Rings, Advances in Mathematics of Communications 6,pp. 39-63, 2012.

[20] S. Jitman, E. Sangwisut and P. Udonkavanich, The Gray Image of skew-constacyclic codes over $\mathbb{F}_{p^m}+u\mathbb{F}_{p^m}+\cdots+u^{e-1}\mathbb{F}_{p^m}$, Chanchuri journal of Mathematics 6,pp. 1-15, 2014.

[21] X. Liu and X. Xu, Cyclic and negacyclic codes of length $2p^s$ over $\mathbb{F}_{p^m}+u\mathbb{F}_{p^m}$, Acta Mathematica Scientia , 34 B (3): 829-839, 2014.

[22] B. R. McDonald, Finite Rings with Identity, Marcel Dekker Press, New York, 1974.

[23] A. Melakhessou, N. Aydin and K. Guenda, $\mathbb{Z}_q(\mathbb{Z}_q+u\mathbb{Z}_q)-$Linear Skew Constacyclic Codes, arXiv preprint arXiv:1803.09316, 2018.

[24] S. Minjia, W. Rongsheng, L. Yan and P. Sol, Two and three weight codes over $\mathbb{F}_p+u\mathbb{F}_p$, Cryptography and communications pp 1-10, 2016.

[25] R. DastBasteh, S. H. Mousavi and J. Haghighat, Characterization of the Skew cyclic codes over $\mathbb{F}_p+v\mathbb{F}_p$, Europ. J. Combinatorics 22, pp. 983-997, 2016.

[26] I. Siap, T. Abualrub, N. Aydin, and P. Seneviratne, Skew cyclic codes of arbitrary length, Int. J. Inf. Coding Theory, (2), pp.10-20, 2011.

[27] A. Sharma and M. Bhaintwal, On skew cyclic codes over $GR(4,2)+uGR(4,2)$, Seventh International Workshop on Signal Design and Its Applications in Communications, (3), 2015.

[28] A. Sharma and M. Bhaintwal, A class of skew-constacyclic codes over $\mathbb{Z}_4+u\mathbb{Z}_4$, Int. J. Information and Coding Theory, (3), 2017.

[29] Z.X. Wan, Lectures on Finite Fields and Galois Rings, World Scientific Pub Co Inc(2003).

[30] J. Wolfmann, Negacyclic and cyclic codes over $\mathbb{Z}_4$, IEEE Trans. Inform. Theory (45), pp. 2527-2532, 1999.

[31] B. Yildiz and S. Karadeniz, Linear codes over $\mathbb{Z}_4+u\mathbb{Z}_4$, MacWilliams identities, projections, and formally self-dual codes, Finite Fields Appl. 27, pp. 24-40, 2014.

Efficient Hardware Implementation of Elliptic Curve Diffie-Hellman Key Exchange Protocol

SAOUDI Mohamed*, KERMICH Akram, ZEBDA abdelfatah, ALLAILOU Boufeldja
Department of Electronics
ESACH, Algiers, Algeria
*saoudimohamed26@gmail.com

***Abstract*—The aim of the present work is the hardware implementation of the elliptic curve Diffie-Hellman (ECDH) key exchange protocol on a reconfigurable circuit of type FPGA at the register-transfer level (RTL). Compared to the standard Diffie-Hellman (DH), based on exponentiation in a finite field, ECDH is known to provide equivalent level of security with lower number of bits used. Reduced bit usage implies less power and logic area are required to implement this cryptographic scheme. This is particularly important in secure embedded system, where a high level of security is required, but with low power consumption. The results show that ECDH can be implemented on FPGA with convincing performances in comparison with other published works.**

***Index Terms*—ECDH, Diffie-Hellman, FPGA, Register-Transfer level, Elliptic Curve.**

I. Introduction

Cryptography has become nowadays a vital tool to ensure the security of the vertiginous growth in the number of connected device via internet. Secret key cryptography is the most popular approach to ensure the confidentiality over a computer network. In fact, the majority of tools provided for this purpose (e.g. Secure Sockets Layer (SSL), Secure Shell (SSH), Ipsec, etc.) rely on the use of symmetric ciphering algorithm like Advanced Encryption standard (AES). This is due to the high speed and the reduced time of ciphering of such algorithm in comparison with their asymmetric counterparts.

The main drawback of the symmetric cryptography is key sharing. For instance, exchanging the key over a public channel would compromise the whole security of the crypto-system. Traditionally, secure encrypted communication between two parties required that they first exchange keys by some secure physical channel, such as paper key lists transported by a trusted courier. In 1976, Whitfield Diffie and Martin Hellman published a paper [1] where they presented their scheme, named after them Diffie-Hellman (DH), for securely exchanging cryptographic keys over a public channel.

Elliptic-curve Diffie-Hellman (ECDH) is an anonymous Key agreement protocol that allows two parties, each having an elliptic-curve public-private key pair, to establish a shared secret over an insecure channel. It is a variant of the Diffie-Hellman protocol using elliptic-curve cryptography (ECC). It was first introduced in 1986 by Victor S. Miller [2].

The use of Field Programmable Gates Arrays (FPGA) for cryptographic applications is highly attractive, especially for embedded secure systems where high performances are required at low power consumption. Therefore, several FPGA-based efficient ECC hardware architectures and elliptic curve cryptographic processors have been presented in the literature ([3], [4], [5] and [6]). The aim of the presented work is the implementation, in an efficient way, of a high performance version of ECDH in the Xilinx Virtex 6 FPGA over the finite binary Galois Field $GF(2^{163})$.

In order to give a clear presentation of our work, this paper is structured as following; After an introduction, a brief review of the mathematical background of ECC is given. Then, we present the cryptographic scheme for the ECDH key exchange protocol. Then, After that we present the proposed architecture of ECDH to be implemented in FPGA. We terminate this paper by giving the results of the implementation by comparing it with existing implementations in literature.

II. Related works

Several FPGA-based efficient ECC hardware architectures and elliptic curve cryptographic processors have been presented in the literature. In [7], Ghanmy proposed ECC processor over $GF(2^{163})$ on an FPGA platform for wireless sensor networks (WSN). Reaz's design [5] can perform ECC over $GF(2^{131})$ and $GF(2^{163})$ on Altera FPGAs. Hasan and Benaissa [6] implemented their ECC processor using the μ-coding technique on Xilinx Spartan-3 FPGAs over $GF(2^{131})$, $GF(2^{163})$, $GF(2^{283})$ and $GF(2^{571})$. An ASIC implementation of an elliptic curve crypto-processor over $GF(2^{163})$ is presented in [8], where they used an ASIC CMOS 45 nm technology as a hardware platform. Shieh [9], Park et al. [10] also proposed their ECC processor over a binary field using Xilinx FPGAs.

III. Elliptic Curve Algebra

In a nutshell, an elliptic curve is a cubic bi-dimensional curve defined by the following relation between the x and y coordinates of any point on the curve:

$$y^2 + xy = x^3 + ax + b \tag{1}$$

Where a and b are arbitrary parameters that define the specific curve used. For a chosen pair (a, b) we can define a *group* structure on it. To do so we define an internal composition rule which satisfies the following three proprieties : *Associativity*, *Identity* and *Inverse* [11]. Even more, if we define a second composition rule over the aforementioned group having the

same proprieties as the first composition rule, we get an algebric structure called *Field* [11]. More precisely, elliptic curves are defined over a finite field called Galois Field. A Galois field denoted normally as $GF(q = p^m)$ is said to be a binary field or characteristic-two finite field if $q = 2^m$.

A non-supersingular elliptic curve E over $GF(2^m)$ in affine coordinates is the set of solutions to the equation 1 where x,y,a,$b \in GF(2^m)$, $b \neq 0$. The coefficients a,b specifying an elliptic curve are typically defined by the NIST standard.

The two essential arithmetic procedures defined on the finite field of elliptic curves $GF(2^m)$ are : the Point Addition (*PA*) and the Point Doubling (*PD*). For a given two points $P = (x_1, y_1)$ and $Q = (x_2, y_2)$ their *PA* R can be found by:

$$R(x_3, y_3) = P(x_1, y_1) + Q(x_2, y_2) \quad (2)$$

$$x_3 = \lambda^2 + \lambda + x_1 + x_2 + a \quad (3)$$

$$y_3 = \lambda(x_1 + x_3) + x_3 + y_1 \quad (4)$$

where $\lambda = (y_2 + y_1)/(x_2 + x_1)$. For *PD* we use:

$$R(x_3, y_3) = 2P(x_1, y_1) \quad (5)$$

$$x_3 = \lambda^2 + \lambda + a = x_1^2 + b/x_1^2 \quad (6)$$

$$y_3 = x_1^2 + \lambda x_3 + x_3 \quad (7)$$

where $\lambda = (x_1 + y_1/x_1)$.

IV. Elliptic Curve Diffie-Hellman

The ECDH cryptographic scheme is shown in figure 1 and is given below:

1) Before starting a communication, Alice and Bob have to get agree, in the public channel, on the parameters of the elliptic curve EC and a point P on this curve, i.e : the coefficients a and b from equation 1, the characteristic polynomial of the field $GF(2^m)$ and the coordinates (x, y) of the point P;
2) Alice generates a secret random private secret k_A;
3) Then she computes $k_A^{pu} = k_A * P$, where $*$ denotes the scalar multiplication in $GF(2^m)$ which could be achieved by using the two arithmetic procedures *PA* and *PD* described in the section III.
4) Bob executes the same actions 1 and 2 to get K_B^{pu};
5) At this point, Alice and Bob exchange with each other K_A^{pu} and K_B^{pu};
6) Alice and Bob can now compute the Secret Symetric Key $k = k_B * k_A^{pu} = k_B * k_A * P$.

The core of ECDH is the scalar multiplication, which computes $\alpha * P$ using only the arithmetic procedures *PA* and *PD*, for example:

$$7 * P = (2P((2P) + P)) + P \quad (8)$$

For a given $Q = \alpha * P$, the problem of calculating α from the points P and Q is called the discrete logarithm problem over the elliptic curve (ECDLP) which is the hard problem underpinning elliptic curve cryptography. Despite almost three decades of research, mathematicians still haven't found an algorithm to solve this problem that improves upon the naive approach. In other words, unlike with factoring (Classical DH), based in currently understood mathematics, there doesn't appear to be a shortcut that will help to find α in a reduced time. This means that for numbers of the same size, solving ECDLP is significantly harder than factoring. Since a more computationally intensive hard problem means a stronger cryptographic system, it follows that elliptic curve cryptograms are harder to break than the ones based on modular exponentiation like RSA and DH [12].

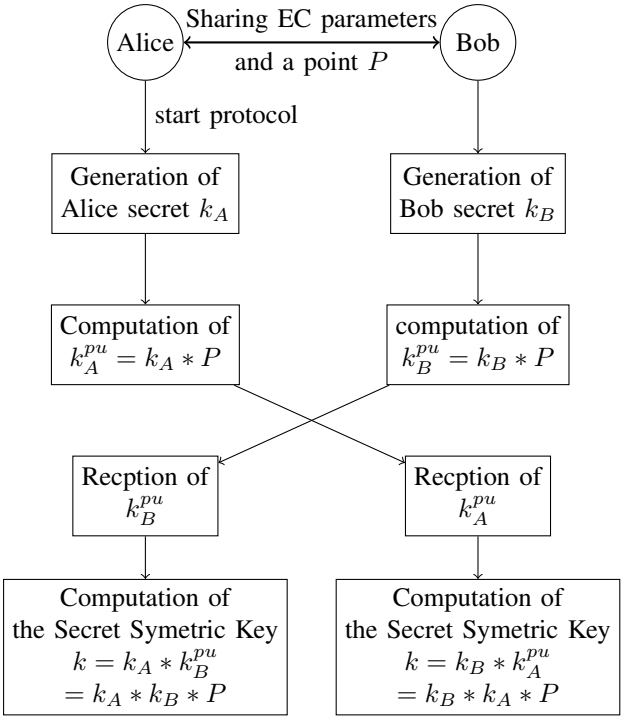


Fig. 1. ECDH key exchange protocol

In 2000, FIPS-2 was recommended with 10 finite fields: 5 prime fields, and 5 binary fields. The binary fields are $GF(2^{163})$, $GF(2^{233})$, $GF(2^{283})$, $GF(2^{409})$ and $GF(2^{571})$ [13]. Prime fields $GF(p)$ and binary fields $GF(2^m)$ of similar size are considered to provide almost the same level of security [14]. Table I compares symmetric cipher key length, and key lengths for PKC such as RSA, Diffie-Hellman (DH), and ECC (both prime and binary fields). It demonstrates that smaller field sizes can be used in ECC than in RSA and DH systems at a given security level. ECC is many times more efficient than RSA and DH for either private-key operations (such as signature generation and decryption) or public-key operations (such as signature verification and encryption).

V. Proposed architecture

As mentioned before, The core of the ECDH is the scalar multiplication (figure 2), therefore, a high importance is given to the proposed FPGA architecture implementing this module. The scalar multiplication module contains two main components. Each one of them ensure either the *PA* or the *PD* procedures. From equations 3, 4, 6 and 7, we can see

TABLE I
COMPARISON OF KEY LENGTH FOR EQUIVALENT SECURITY OF SYMMETRIC-KEY AND PUBLIC-KEY CRYPTOGRAPHY [15]

Summytric key	Example Alg.	RSA and DH	ECC in $GF(p)$	ECC in $GF(2^m)$
112	Triple-DES	2048	224	233
128	AES Small	3072	256	283
192	AES Medium	8192	384	409
256	AES Large	15360	521	571

that the operations needed to implement *PA* and *PD* are : addition, multiplication, squaring and division. It is known that the addition in $GF(2^m)$ is equivalent to a simple *xor* in either hardware or software. For the remaining operations, this section gives in details the algorithms and methods used to implement them. It is useful to mention that all of the operations are executed using the polynomial representation of elements in $GF(2^m)$.

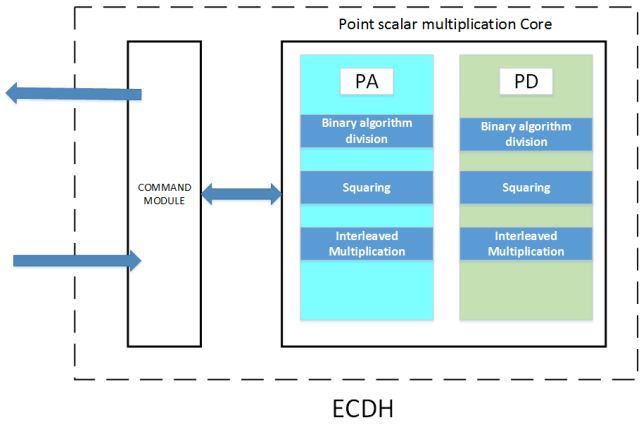


Fig. 2. proposed hardware architecture for ECDH

A. Multiplication in $GF(2^m)$

Multiplication in $GF(2^m)$ with the interleaved modular reduction algorithm is a well-known algorithm for hardware implementation [16]. It computes the product of two polynomials then applies modular reduction, and its operation is different from simple integer multiplication. The algorithm 1 describes in details the interleaved modular reduction.

B. Squaring in $GF(2^m)$

Squaring in $GF(2^m)$ has less computation complexity than polynomial multiplication because it can be achieved by setting a 0 bit between consecutive bits of the operand, as shown in figure 3.

C. Division in $GF(2^m)$

Division in $GF(2^m)$ is the most expensive operation for implementing ECC over a binary field. The quotient of two polynomials in $GF(2^m)$ can be computed using the binary version of the binary algorithm that is used for calculation of

Algorithm 1 Multiplication in $GF(2^m)$ with interleaved modular reduction

Input : $P(x)$, $Q(x)$ and $f(x) \in GF(2^m)$
Output : $R(x) = P(x)Q(x) \mod f(x)$
Initialization : $R_v = 0$; $P_v =' 0' \& P(x)$
for $i = (m-1)$ **to** 0 **do**
  if $Q(i) =' 1'$ **then**
    $R_v = R_v x \oplus Q_v$;
  else
    $R_v = R_v x$;
  end if
  if $R_v(m) =' 1'$ **then**
    $R_v = R_v \oplus f(x)$;
  end if
end for
Return $R(x)$;

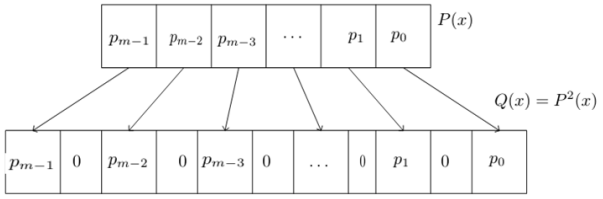


Fig. 3. Squaring a binary polynomial $P(x)$

the great common divider (GCD) for polynomials. The binary algorithm for computing $R(x) = P(x)Q^{-1}(x) \mod f(x)$ is described in algorithm 2.

VI. FPGA IMPLEMENTATION RESULTS AND PERFORMANCE ANALYSIS

This section presents the hardware implementation results of the proposed architecture. We have implemented and tested our design on a modern Xilinx Virtex-6 (XC6VLX240T) FPGA. All VHDL modules are extensively simulated using both Isim and ModelSim, and synthesized using Xilinx ISE 14.7 synthesis technologies. The parameters for the elliptic curve used are taken from the NIST standard and are given in table II. We choose to work with the irreducible polynomial $f(x) = x^{163} + x^7 + x^6 + x^3 + 1$ over the field $GF(2^{163})$.

TABLE II
NIST-RECOMMENDED ELLIPTIC CURVES OVER $GF(2^{163})$ [13]

K-163: $m = 163$, $f(x) = x^{163} + x^7 + x^6 + x^3 + 1$, $a = b = 1$, $h = 2$					
n=0x 4	00000000	00000000	00020108	A2E0CC0D	99F8A5EF
x=0x 2	FE13C053	7BBC11AC	AA07D793	DE4E6D5E	5C94EEE8
y=0x 2	89070FB0	5D38FF58	321F2E80	0536D538	CCDAA3D9

A. Implementation of PA and PD

To implement the PA core we needed to infer a module for multiplication, a module for squaring and another one for division, in addition to a Finite State Machine (FSM)

Algorithm 2 Binary algorithm for polynomials division in $GF(2^m)$

Input : $P(x)$, $Q(x)$ and $f(x) \in GF(2^m)$
Output : $R(x) = P(x)Q^{-1}(x) \mod f(x)$
Initialization : $a = f$, $b = Q_v$, $c = 0$, $d = P_v$, $\alpha = m$ and $\beta = m - 1$
while $\beta > 0$ **do**
  if $b(0) = 0$ **then**
    $b = b << 1$;
    $d = d/x \mod (f)$;
    $\beta = \beta - 1$;
  else
    $old\_\beta = \beta$;;
    $b = a \oplus b << 1$;
    $d = (c \oplus d)/x \mod (f)$;
    if $\alpha > \beta$ **then**
      $\beta = \alpha - 1$; $\alpha = old\_\beta$;
      $c = d$;
    else
      $\beta = \beta - 1$;
    end if
  end if
end while
$R(x) = c$;
Return $R(x)$;

for the control of the whole operation. The same modules were inferred to implement the PD core but with a different FSM. Result of implementation are given in table III. Useful to notice that the time row in the table correspond to the time needed to complete the PA or PD procedure at a frequency of 200 Mhz.

TABLE III
RESOURCES UTILIZATION AND PERFORMANCES OF PA AND PD IMPLEMENTATION

	PA	PD
Slice registers	4855 (1%)	4367(1%)
Slice LUT	2817 (1%)	2661 (1%)
Max frequency (Mhz)	325	325
Time (µs)	2.54	3.38

B. Implementation of the scalar multiplication core

Using PA and PD module, we have succeeded to implement the scalar multiplication core. The proposed design contains a PA module and PD module which are controlled by an FSM. Table IV summarizes the results of the scalar multiplication core implementation in comparison with a recent work [11], where the authors implemented another architecture for the scalar multiplication module over Binary Field $GF(2^{163})$. Worth to mention that the FPGA used in [11] is more modern and possibly offers a higher work frequency. Nevertheless, as shown in table IV our design takes less time to compute the scalar multiplication.

TABLE IV
SCALAR MULTIPLICATION RESOURCES UTILIZATION AND PERFORMANCES : COMPARAISON BETWEEN OUR WORK AND [11]

	Our work	Hossain *et al.* [11]
FPGA	Virtex-6	Kintex-7
Slice registers	11217 (3%)	6620(1%)
Slice LUT	6560 (4%)	7963 (3%)
Frequency (Mhz)	200	306.48
Time (µs)	766	1060

C. implemntation of ECDH

With scalar multiplication core ready to use, the implementation of ECDH only needed an appropriate FSM. Therfore the resources utilization is approximately equal to the one shown in table IV.

VII. CONCLUSION

An efficient implementation of ECDH in FPGA has been presented in this work. A high-performance cores for computing the PA and PD procedures over $GF(2^{163})$ were designed. The implementation results have shown that our proposed architecture present two main advantages : a low resource utilization which makes it ideal for embedded system; and reduced time of calculation which makes this solution a good candidate for hardware acceleration of various internet security.

REFERENCES

[1] W. Diffie, M. Hellman, "New Directions in Cryptography," IEEE trans. on Information Theory, pp. 644–654, November 1976.
[2] V. S. Miller, "Use of Elliptic Curves in Cryptography," Advances in Cryptology – CRYPTO'85, pp. 417–426, 1986.
[3] G. Sutter, J. Deschamps, J. Imana, " Efficient Elliptic Curve Point Multiplication Using Digit-Serial Binary Field Operations," IEEE Trans. on Industrial Electronics, pp. 217–225, 2013.
[4] W. Chelton, M. Benaissa, "Fast Elliptic Curve Cryptography on FPGA," IEEE Trans. on Very Large Scale Integration (VLSI) Systems, pp. 198–205, 2008.
[5] M. B. I. Reaz, J. Jalil, H. Husain, F.H. Hasim, "FPGA implementation of elliptic curve cryptography engine for personal communication systems," Tran. on Circuits and Systems, pp. 82–91, 2012.
[6] M. Hassan, M. Benaissa, "Efficient time-area scalable ECC processor using µ-coding technique,"Third International Workshop, WAIFI, Arithmetic of Finite Fields, pp. 250—268, 2010.
[7] N. Ghanmy, L. C. Fourati, L. Kamoun, "Elliptic curve cryptography for WSN and SPA attacks method for energy evaluation," Journal of Networks, pp. 2943–2950, 2014.
[8] M. Machhout, Z. Guitouni, K. Torki, L. Khriji, R. Tourki, "Coupled FPGA/ASIC implementation of elliptic curve crypto-processor," International Journal of Network Security its Applications (IJNSA), pp. 100—112, 2010.
[9] M.D. Shieh, J.H. Chen, W.C. Lin, C.M. Wu, "An efficient multiplier/divider design for elliptic curve cryptosystem over $GF(2^m)$," Journal of Information Science and Engineering, pp. 1555—1553, 2009.
[10] J. Park, J.T. Hwang, "FPGA and ASIC implementation of ECC processor for security on medical embedded system," The Third International Conference on Information Technology and Applications (ICITA'05), pp. 547—551, Washington, DC, USA, 2005. Computer Society
[11] M. S. Hossain, E. Saeedi, Y. Kong, " High-performance FPGA Implementation of Elliptic Curve Cryptography Processor over Binary Field $GF(2^{163})$," In Proceedings of the 2nd International Conference On Information Systems Security and Privacy, pp 415–422, 2016.

[12] M. Amara, A. Siad, "Elliptic Curve Cryptography And Its Applications," 7th International Workshop on Systems, Signal Processing and their Applications (WOSSPA), Tipaza, Algeria, 2011.
[13] NIST-National Institute of Standards and Technology, Digital Signature Standard, FIPS Publication 186-2, 2000.
[14] N. Koblitz, A. Menezes, S. Vanstone, "The state of elliptic curve cryptography," Des. Codes Cryptography, pp. 173–193, 1987.
[15] D. Hankerson, A. Menezes, S. Vanstone, " Guide to Elliptic Curve Cryptography," Springer-Verlag New York, Inc., Secarus, NJ, USA, 2003.
[16] J. Wolkerstorfer, " Dual-field arithmetic unit for $GF(p)$ and $GF(2^m)$," CHES, Lecture Notes in Computer Science, pp. 500–514, 2002.

Authentication, Ciphering & Security in Modern Mobile Network

S.S.Belaifa
Technology/ T.NOC.Transmission
Djezzy Telecom Algeria

***Abstract* — In This paper we present the notion of authentication , Ciphering and security for Mobile network , the technologies involved are 2G, 3G et 4G .**
We focus our study on GSM system. In General these parameters are defined by constructors; however security is managed by IT.SECURITY department.

***Keywords* — Signaling, Authentication, Ciphering & IT.Security.**

I. INTRODUCTION

The need to protect valuable information is as old as history. As far back as Roman times, Julius Caesar saw the need to encrypt messages by means of shift alphabetic letters. Cryptology has developed over the centuries from an art, in which only few were skillful, into a science.
The cryptology is the studies of sciences of communications of coded messages read only in the destination. The cryptosystem is a process of encryption and decryption use to transmit and receive secret information. The key cryptosystem is a code enables to encrypt a message during his transmission or decrypt at the destination [1]. Many people regard the "Communication Theory and Secrecy Systems" paper, by Claude Shannon in 1949, as the foundation of modern cryptology.
In 1976, the paper "New Directions in Cryptography," by Whitfield Diffie and Martin Hellman, caused a shock in the academic community. This seminal paper showed that people who are communicating with each other over an insecure line can do so in a secure way with no need for a common secret key. In Shannon's world of secret key cryptography this was impossible, but in fact there was another cryptologic world of public-key cryptography, which turned out to have exciting applications in the real world [2]. The 1976 paper and the subsequent paper on the RSA cryptosystem in 1978, Rabin in 1979 and Merkle-Hellman in 1978 also showed something else: mathematicians and computer scientists had found an extremely interesting new area of research. From the notion of public-key cryptography, information security was born as a new discipline and it now affects almost every aspect of life.

In this paper we present a notion of security in Mobile Network: 2G, 2.5G, 3G and 4G, for Packet Switch or Circuit Switch. We focus on study on 2G in order to understand the basic of security.
The processes of security for 2.5G, 3G and 4G systems are not presented in this paper, but are the same philosophy as 2G systems

Three aspects are treated: authentication, confidentiality and integrity protection of signaling. Authentication consists to check user identity. Confidentiality is to return information incomprehensible for others users. Protection of signaling data integrity consist to determine if during the exchange there is no deterioration. The purpose of signaling is management, organization and transport of all traffic in the network, so the network handles the traffic via its signaling. The signaling system #7 (SS7) is a set of protocols of telephony signaling which are used in majority of telephony networks in the world. The protocols in seven layers are presented in Figure 4.

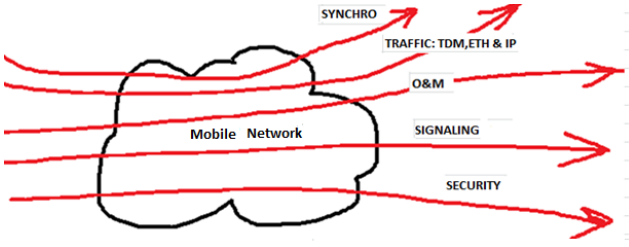


Fig.1. the 5 essentials paths END to END in MOBILE NETWORK

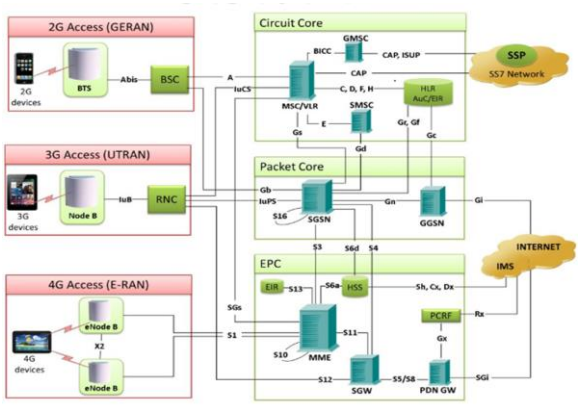


Fig.2. Equipment's and Interfaces in 2G, 2.5G, 3G and 4G

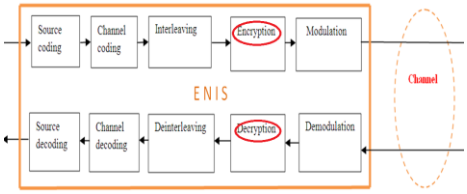


Fig.3.Ciphering in telecommunication s Equipment's : UE, BTS, NODEB, ENODE, BSC, RNC, ……

The Authentication, Cyphering, and Security are defined by constructors of telecommunication equipment.

In practice security is the responsibility of IT security department:

- IT.SECURITY NETWORK.
- IT.SECURITY SYSTEMS.

II AUTHENTIFICATION, CYPHERING & SECURITY IN GSM NETWORK

We define also the associated equipment as: MS : Mobile Station or the mobile phone, BTS : Base Transceiver Station, BSC : Base Station Controller. MSC : Mobile services Switching Center and different interfaces : Um, Abis and A.

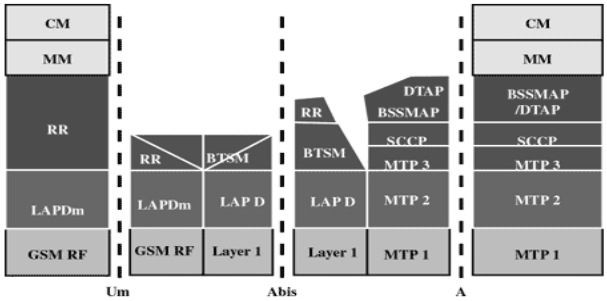


Fig. 4. GSM Signaling Protocol Stack

Radio protocol sublayer functions at physical layer between the MS and BTS is presented as below:

- Full or Half duplex access
- SDMA, FDMA and TDMA.
- Bursting and Framing.
- Synchronizing the MSs and path delays corrections
- Frequency Correction.
- Coding, FEC, CRC, data interleaving and encryption.
- Error detection and correction.
- GMSK digital modulation and transmission.
- Demodulation and reception.
- **Decrypting** et decoding.

The cyphering is in physical layer and layer 5(BSSMAP).

Authentication is in layer 5 (DTAP) and layer 6 MM (Mobility Management) with:

- Registration Update
- **Authentication and identification method IMSI**.
- Use of TMSI allocated by VLR in place of IMSI at HLR.
- Maintaining reliable communication to upper layers.

A. Authentication and key generation with A3/A8 Algorithm

The authentication center (AuC) is a function to authenticate each SIM card that attempts to connect to the GSM core network (typically when the phone is powered on). Once the authentication is successful, the HLR is allowed to manage the SIM and services described above. An encryption key is also generated that is subsequently used to encrypt all wireless communications (voice, SMS, etc.) between the mobile phone and the GSM core network. The A3/A8 used for authentication and key generation also A5 algorithm used for ciphering. A3 and A8 both take a 128 bits key (Ki) and a 128 bits challenge (RAND) as inputs. A3 produces a 32 bits response (SRES) and A8 produces a 64 bits session key (Kc).
A3/A8 use COMP128-1 algorithm describe as below :

```
Soient les tables compressées  T0[512], T1[256], T2[128], T3[64]
et T4[32] :

comp128 : RAND, Ki -> SRES, Kc
{
 x[32]:      array of bytes
 bit[128]:   array of bits
 m, n, y, z: integers

 x[16..31] := RAND
 for i := 1 to 8
   x[0..15] := Ki
   for j := 0 to 4
     for k := 0 to 2^j-1
       for l := 0 to 2^(4-j)-1
         m := l + k * 2^(5-j)
         n := m + 2^(4-j)
         y := (x[m] + 2 * x[n]) mod 2^(9-j)
         z := (2 * x[m] + x[n]) mod 2^(9-j)
         x[m] := Tj[y]
         x[n] := Tj[z]
   for j := 0 to 31
     for k := 0 to 3
       bit[4 * j + k] := x[j]^(3-k)
   if i < 8
     for j := 0 to 15
       for k := 0 to 7
         x[j + 16]^(7-k) := bit[((8 * j + k) * 17) mod 128]
 SRES := bit[0..31]
 Kc := bit[74..127]
}
```

B. Ciphering with A5/1 algorithm

A5/1 is the symmetric cipher used for encrypting over-the-air transmissions in the GSM standard. A5/1 is used in most European countries, whereas a weaker cipher, called A5/2, is used in other countries. The description of

A5/1 was first kept secret but its design was reversed engineered in 1999 by Briceno, Golberg, and Wagner. A5/1 is a synchronous stream cipher based on linear feedback shift registers (LFSRs). It has a 64-bit secret key. A GSM conversation is transmitted as a sequence of 228-bit frames (114 bits in each direction) every 4.6 millisecond. Each frame is xored with a 228-bit sequence produced by the A5/1 running-key generator. The initial state of this generator depends on the 64-bit secret key, K, which is fixed during the conversation, and on a 22-bit public *frame number*, F. The A5/1 running-key generator consists of three LFSRs of lengths 19, 22, and 23. Their characteristic polynomials are $X19 + X5 + X2 + X + 1$, $X22 + X + 1$, and $X23 + X15 + X2 + X + 1$. For each frame transmission, the three LFSRs are first initialized to zero. Then, at time $t = 1, \ldots, 64$, the LFSRs are clocked, and the key bit Kt is xored to the feedback bit of each LFSR. For $t = 65, \ldots, 86$, the LFSRs are clocked in the same fashion, but the $(t - 64)$ th bit of the frame number is now xored to the feedback bits.

After these 86 cycles, the generator runs as follows. Each LFSR has a clocking tap: tap 8 for the first LFSR, tap 10 for the second and the third ones (where the feedback tap corresponds to tap 0). At each unit of time, the majority value b of the three clocking bits is computed. A LFSR is clocked if and only if its clocking bit is equal to b. For instance, if the three clocking bits are equal to (1, 0, 0), the majority value is 0. The second and third LFSRs are clocked, but not the first one. The output of the generator is then given by the xor of the outputs of the three LFSRs. After the 86 initialization cycles, 328 bits are generated with the previously described irregular clocking. The first 100 ones are discarded and the following 228 bits form the running-key.

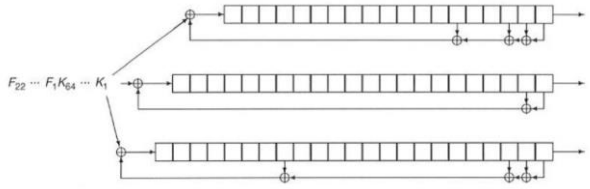


Fig. 5. Initialization of A5/1

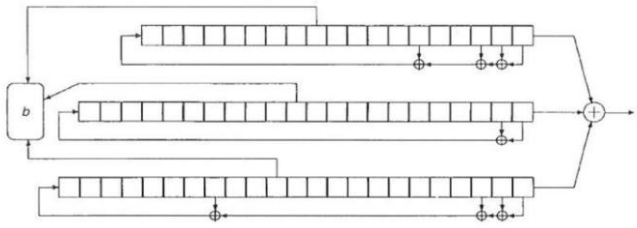


Fig.6. A5/1 running-key generator

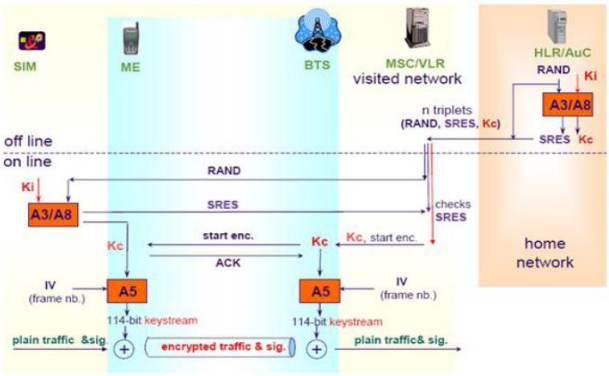


Fig. 7. Authentication and Ciphering in GSM network

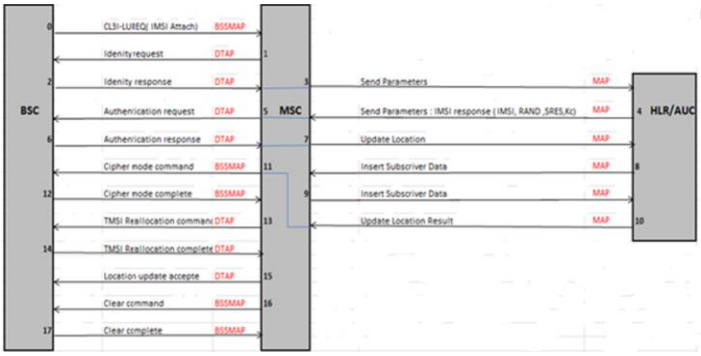
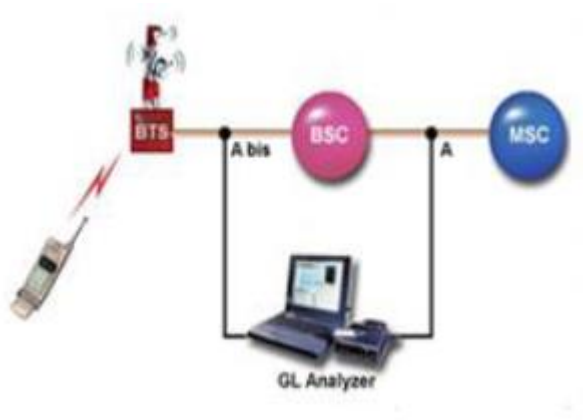


Fig.8. Messages in Location Update Procedure

C. GSM Protocol Analyzer in Core Network

Telecom Network Protocol Analyzer is a Protocol analyzer to analyze a switching and signaling telecommunication protocol between different nodes in PSTN or Mobile telephone networks, such as 2G or 3G GSM networks, and so on. In a mobile telecommunication network it can analyze the traffic between MSC and BSC, BSC and BTS, MSC and HLR, MSC and VLR, VLR and HLR, and so on. Protocol analyzers are mainly used for performance measurement and troubleshooting. For example in GSM, we find authentication and ciphering messages in MAP, DTAP and BSSMAP protocols, especially in Location Update Procedure (see Figure 8). As Example of equipment: Tektronix K15, ACTERNA and *Huawei* Local Maintenance Terminal.



No.	TimeStamp	Msg Interface	Msg Type
1	2015-05-24 12:20:36	>TRC MI FROM A	CM Service Request
2	2015-05-24 12:20:36	<TRC MI TO A	N CONNECT RESP
3	2015-05-24 12:20:36	<TRC MI TO A	Cipher Mode Command
4	2015-05-24 12:20:36	>TRC MI FROM A	Classmark Update
5	2015-05-24 12:20:37	>TRC MI FROM A	Cipher Mode Complete
6	2015-05-24 12:20:37	>TRC MI FROM A	Setup
7	2015-05-24 12:20:37	<TRC MI TO A	Call Proceeding
8	2015-05-24 12:20:37	<TRC MI TO A	Assignment Request
9	2015-05-24 12:20:38	>TRC MI FROM A	Assignment Complete
10	2015-05-24 12:20:42	<TRC MI TO A	Alert
11	2015-05-24 12:20:46	>TRC MI FROM A	HO Performed
12	2015-05-24 12:20:52	<TRC MI TO A	Connect
13	2015-05-24 12:20:53	>TRC MI FROM A	Connect Ack
14	2015-05-24 12:21:40	<TRC MI TO A	Disconnect
15	2015-05-24 12:21:40	>TRC MI FROM A	Release
16	2015-05-24 12:21:40	<TRC MI TO A	Release Complete
17	2015-05-24 12:21:40	<TRC MI TO A	Clear Command
18	2015-05-24 12:21:40	>TRC MI FROM A	Clear Complete

Fig.9. BSSMAP messages in A interface for call

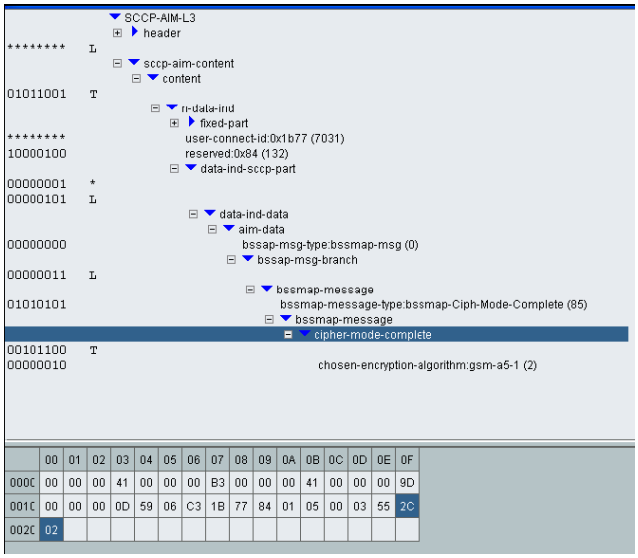


Fig.10 . Choose of A5/1 algorithm in CIPHER-MODE-COMPLETE message (BSSMAP Protocol)

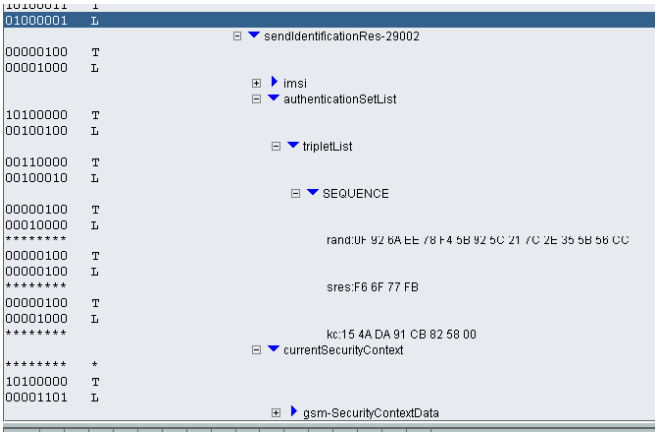


Fig.11. Triplet RAND, SRES and Kc in SEND IDENTIFICATION RSP message (MAP Protocol)

III HANDLE SECURITY IN MOBILE NETWORK OPERATOR

It seems that service IT handle security in IP lever (Router).

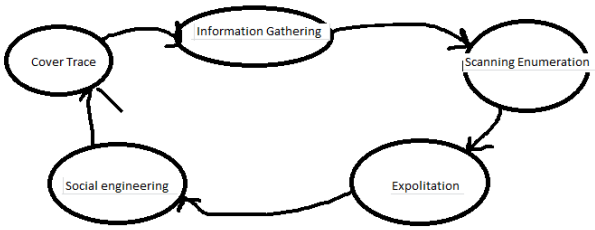


Fig.12. How to start security Project

A. SOC: Service Operations Center

Security operations centers monitor and analyze activity on networks, servers, endpoints, databases, applications, websites, and other systems, looking for anomalous activity that could be indicative of a security incident or compromise. The SOC is responsible for ensuring that potential security incidents are correctly identified, analyzed, defended, investigated, and reported.

Exploitation by METASPLOIT (over Klinux system)

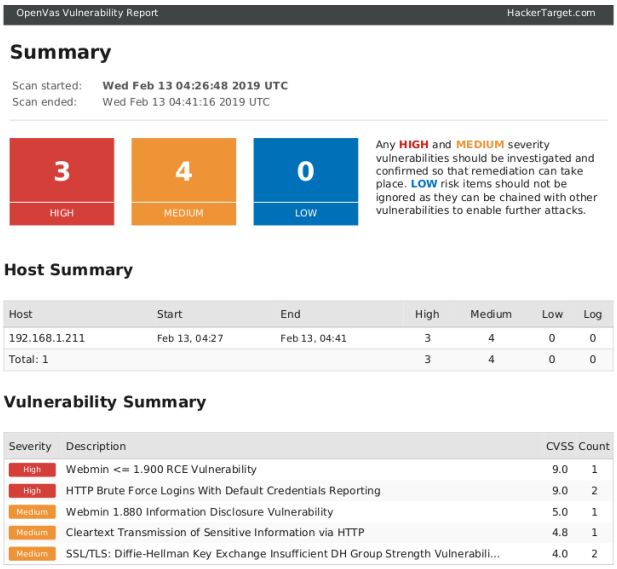
Metasploit helps security teams do more than just verify vulnerabilities, manage security assessments, and improve security awareness.

- A **port scanner** is an application designed to probe a server or host for open ports

21 /TCP open FTP.
22/TCP open SSH.
23 / TCP open TELNET.
80/TCP open HTTP.
43/TCP open HTTPS.

- A **vulnerability scanner** is a computer program designed to assess computers, networks or applications for known weaknesses

In below an example of vulnerability scanner result



OpenVas Vulnerability Report — HackerTarget.com

Summary

Scan started: **Wed Feb 13 04:26:48 2019 UTC**
Scan ended: Wed Feb 13 04:41:16 2019 UTC

3	4	0
HIGH	MEDIUM	LOW

Any **HIGH** and **MEDIUM** severity vulnerabilities should be investigated and confirmed so that remediation can take place. **LOW** risk items should not be ignored as they can be chained with other vulnerabilities to enable further attacks.

Host Summary

Host	Start	End	High	Medium	Low	Log
192.168.1.211	Feb 13, 04:27	Feb 13, 04:41	3	4	0	0
Total: 1			3	4	0	0

Vulnerability Summary

Severity	Description	CVSS	Count
High	Webmin <= 1.900 RCE Vulnerability	9.0	1
High	HTTP Brute Force Logins With Default Credentials Reporting	9.0	2
Medium	Webmin 1.880 Information Disclosure Vulnerability	5.0	1
Medium	Cleartext Transmission of Sensitive Information via HTTP	4.8	1
Medium	SSL/TLS: Diffie-Hellman Key Exchange Insufficient DH Group Strength Vulnerabili...	4.0	2

Nmap (Network Mapper) is a free and open-source network scanner , Nmap is used to discover hosts and services on a computer network by sending packets and analyzing the responses.

Nmap provides a number of features for probing computer networks, including host discovery and service and operating system detection. These features are extensible by scripts that provide more advanced service detection, vulnerability detection, and other features.

- Data base failure : www.exploit-db.com

REFERENCES

[1] Alain Kraus, " Cours de cryptographie " Université Pierre et Marie Curie 2012 /2013.

[2] Henk C.A. van Tilborg, " Encyclopedia of cryptography and security " Eindhoven University of Technology The Netherlands 2005 Springer Science Business Media.

[3] Whitfield diffie and martine hellman, " New directions in Cryptography» 1976 IEEE transaction on information theory.

[4] X. Lagrance P. Godlewski and S. Tabbane, " Réseaux GSM" 3rd ed Hermes sciences publications 2000.

[5] S.S. Belaifa," Information theory and signal processing in GSM Network" 3rd International Conference on Information and Electronics Engineering (ICIEE 2013).

[6] Claude Shannon "Communication theory and secrecy systems 1949".

[7] Mohamed Lakri "Hacking and security level 01", 05-06 August 2018 ,

Hardware Acceleration of AES Cryptographic Algorithm for IPsec

BENHADDAD Omar Hocine*, SAOUDI Mohamed, DROUICHE Amine, RABIAI Mohamed, ALLAILOU Boufeldja
Department of Electronics
ESACH, Algiers, Algeria
*omar.hocine.benhaddad@gmail.com

***Abstract*—This research considers the offloading of the IPsec packet encryption algorithm into an FPGA by proposing a hardware acceleration of the AES cryptographic algorithm for IPsec. We point out the benefits of relying on HW acceleration in terms of speed and energy efficiency for applications like IPsec.**

We present the description of the architecture of the proposed solution, the simulation results of our implementation of the AES algorithm in ECB (Electronic Code Book) mode. We also present the integration of the encryption core with the IPsec subsystem through a PCIe bus interface so that the resulting implementation is interoperable with other systems.

***Index Terms*—IPsec, FPGA, AES, RIFFA, cryptography.**

I. Introduction

The volume of data exchanged over networks has been increasing over the past decade. An increase that goes along with the need to protect this data at a much higher rate as it is more and more exposed on public networks. Sensitive data should be secured seamlessly and the process shouldn't act as a bottleneck. In 1998, IPsec was developed by the IETF (Internet Engineering Task Force). It is now one of the most popular solutions to secure data at the IP layer. The IPSec protocol is almost always integrated into the TCP/IP stack on Operating Systems (Windows, Linux...) but it needs a lot of computational power. One of the most computationally intensive parts is the encryption algorithm which in our case is the AES (Advanced Encryption Standard).

In this paper, we consider the feasibility of offloading AES cryptographic algorithm from software to FPGA connected through a PCIe endpoint to a host computer running on a Linux distribution.

II. Related works

Several papers has been published in the field of hardware acceleration of cryptographic algorithms.

In 2007, Kemsitzer et al [1] achieved a 15.3 Gbps from their implementation of the AES in GCM mode on a Virtex-4 FPGA under a clock rate of 120 Mhz.

In 2011, the implementation of the AES algorithm by Soliman et al [2] reached 74 Gbps on a Virtex-5 FPGA under the clock rate of 557 Mhz.

In 2016, Smekal et al [3] described the AES implementation on Virtex-7 that achieved a 5.1 Gbps throughput under a clock rate of 100 Mhz.

In 2013, Yun Niu et al [4] implemented a design that includes 8 IPsec protocol IP cores and 24 crypto IP cores. The design give the throughput of 11.28 Gbps under a clock rate of 300 Mhz.

III. IPsec

IPsec (Internet Protocol Security) is a set of protocols that uses cryptographic algorithms to ensure private and protected communications on IP networks. It operates on the network layer (3rd layer of the OSI model), therefore preventing the user from reconfiguring applications with IPsec standards on the application layer.

The main purpose of IPsec is to authenticate and to encrypt the data flow between the two participants in order to ensure confidentiality and integrity.

In order to establish an IPsec connexion we need first to exchange the keys through the IKE protocol (Internet Key Exchange) which is used to authenticate the two participants of a secured tunnel by exchanging shared keys. Then the transfer of the data flow can be done through two possible protocols which are AH (Authentication Header) or ESP (Encapsulating Security Payload).

The Figure 1 shows the position of IPsec on the third layer of the OSI model and that we use the PCIe bus to transfer data between the host computer and the FPGA.

IV. AES presentation

The Rijndael AES algorithm was adopted on 26 May 2002 by the NIST to replace the symmetric-key algorithms such as DES or 3DES [5]. The AES algorithm can process data blocks of 128 bits, using cipher keys with lengths of 128, 192 and 256 bits. Both of the keys and the data block are written as matrices, so all the operations are are done on matrices.

The state matrix for the data block consists of 4 rows of bytes, each containing N_b bytes, where N_b is the block length divided by a 32-bit word. Thus we obtain $N_b = \frac{blocklength}{32} = 4$. Depending on the security requirements, we can choose the key length 128 bits, 192 bits or 256 bits which corresponds to the algorithm name "AES-128", "AES-192" or "AES-256".

The AES algorithm consists of a key expansion algorithm that generates the round keys from the primary key. The key length determines the number of rounds N_r in the encryption/decryption process of the AES. The number of rounds

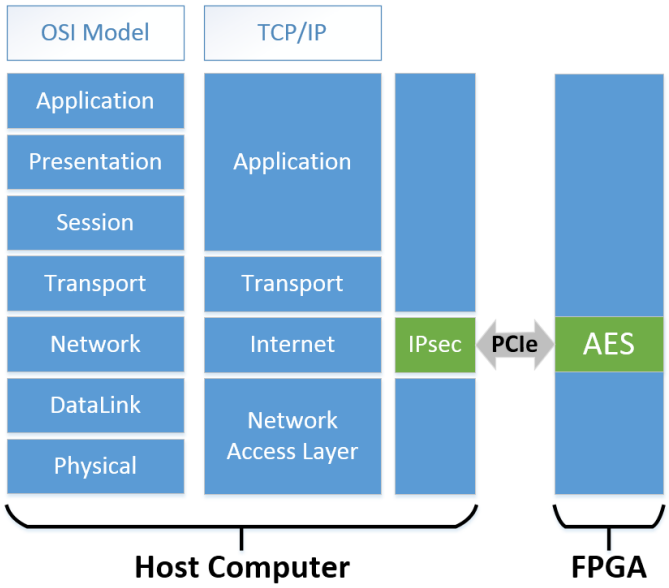


Fig. 1. Communication between IPsec in the host computer part and the AES in the FPGA part through PCIe bus

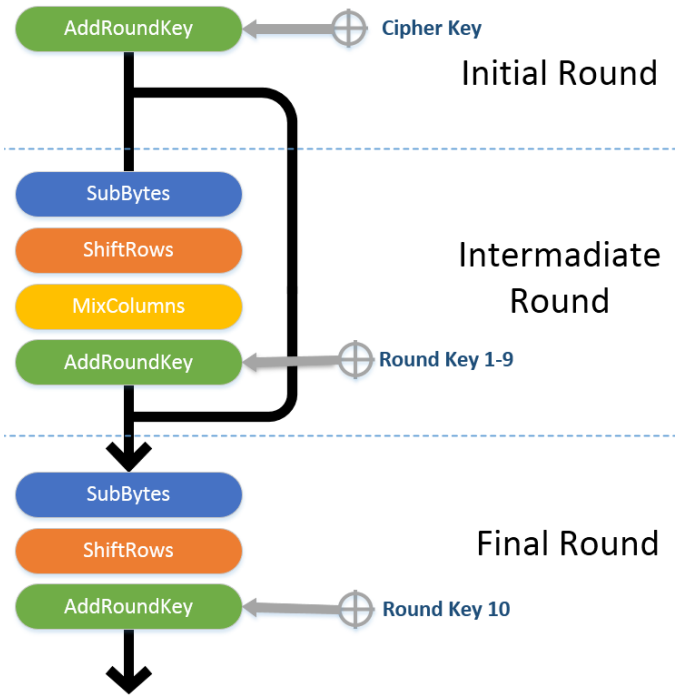


Fig. 2. AES algorithm

for AES-128 is $N_r = 10$ for AES-192 is $N_r = 12$ and for AES-256 is $N_r = 14$. The Figure 2 shows the initial round that adds the primary key to the state matrix of the data block. Intermediate rounds from round 1 to round $N_r - 1$ that consist of a set of four distinct operations including a substitution operation, a shifting rows and a mixing columns operations and finally, adding a round key operation. The final round N_r doesn't contain the mix columns operation.

V. RIFFA 2.0

RIFFA (Reusable Integration Framework for FPGA Accelerators) is a framework that allows to establish a communication between an FPGA and a host PC using PCIe standard. The host PC can run either on Windows OS or Linux OS [6]. The RIFFA framework provides a software API with two main functions "data send" and "data receive" that are written in C/C++, Python, Matlab and Java. Those functions are used for sending and receiving data to/from the FPGA connected to the PCIe bus. A hardware interface that allows the transmission/reception of data through a FIFO interface and a DMA (Direct Memory Access). The user needs to interface his hardware architecture directly on the RIFFA framework in order to communicate between the FPGA and the host PC.

VI. The proposed solution

A. The architecture

In order to accelerate the cryptographic transformation for IPsec, we propose the architecture shown on the Figure 3. It consists of two main parts:

- The host computer comprises the PCIe endpoint, the RIFFA device driver in the Linux Kernel, the RIFFA low level API which provides the software functions "fpga send" and "fpga receive" and finally, the user application software.
- The FPGA comprises a PCIe endpoint, a RIFFA hardware driver, and the user logic which consists of the the implementation of the AES algorithm.

The raw data (the payload) of the IPsec protocol instead of being ciphered in the host PC, are transmitted to the FPGA in order to be ciphered there with an AES algorithm previously implemented in. The data transfer from the host machine to the FPGA is done through the PCIe bus using the RIFFA framework.

B. Finite state machine of the AES-128 algorithm

The FMS of the AES-128 algorithm shown in the Figure 4 consists of 4 states:

1) **Wait for start**: It's the initial state of the FSM. When RST=1, the FSM is reset to this state. It waits for the start signal to begin the process.
2) **Load Key**: Load the key then wait for Ready signal.
3) **Load Data**: Load the data to encrypt/decrypt and wait for ready signal.
4) **Finish process**: When the process is finished, we return to the first state.

C. Finite state machine of the interface between AES-128 algorithm and RIFFA framework

The FSM of the interface between AES-128 and RIFFA hardware driver is shown in the Figure 5. It consists of 6 states:

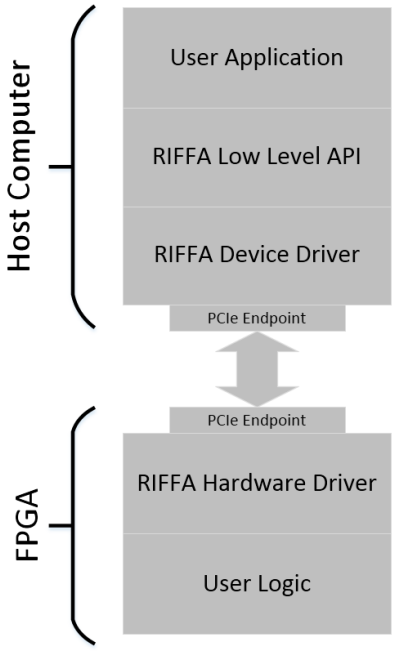


Fig. 3. Architecture proposed to accelerate cryptographic transformation for IPsec

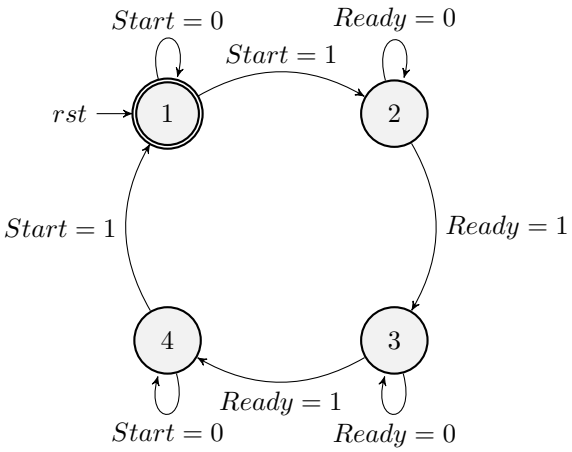


Fig. 4. FSM of the AES-128 algorithm

1) **Wait for Rx**: It's the initial state of the FSM. When RST=1, the FSM is reset to this state. It waits for the signal Rx_En to enable data reception.
2) **Wait for last data**: Reception starts and continues until the last 32 bits word are sent which is indicated by the signal Rx_Last=1. Transition to the next state is then made.
3) **AES enable**: In this state Start signal is set to 1 in order to start the cipher/decipher operation.
4) **Wait result**: Wait for the Finish signal to take the value 1 which indicates the end of the cipher/decipher operation.
5) **Prepare for Tx**: Initialisation of the counter of the words to send before data transmission starts.
6) **Transmit data**: The end of the transmission is indicated by the signal Tx_Last=1.

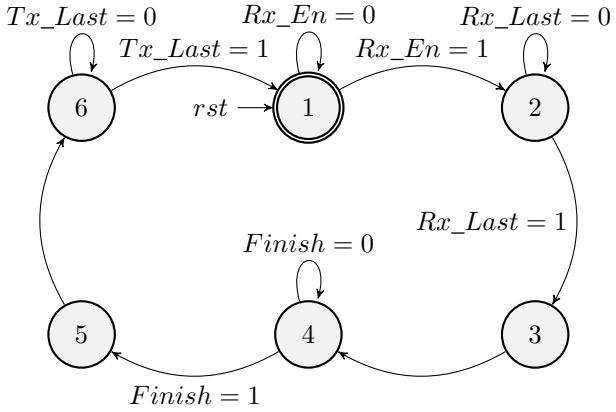


Fig. 5. FSM of the interface between the AES algorithm and RIFFA framework

D. Test bench verification for the AES-128 encryption/decryption algorithm

In order to verify the proper functioning of the AES-128 algorithm in encryption/decryption modes, we compare the results with the following FIPS test vector [7].

- **Primary Key**: 2b7e151628aed2a6abf7158809cf4f3c
- **Plain text**: 6bc1bee22e409f96e93d7e117393172a
- **Cipher text**: 3ad77bb40d7a3660a89ecaf32466ef97

We can notice in the Figure 6 that the result of th encryption is equal to the cipher text FIPS test vector.

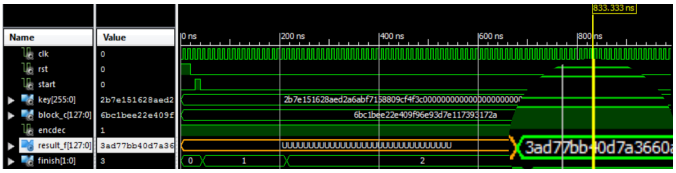


Fig. 6. Test bench of the AES encryption

As well, in the Figure 7 we can notice the result of the decryption is equal to the plain text FIPS test vector.

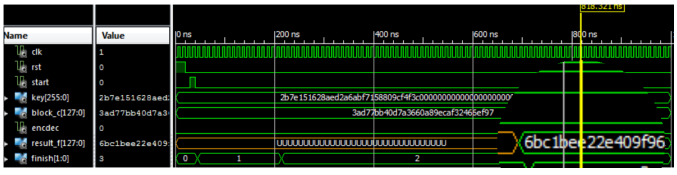


Fig. 7. Test bench of the AES decryption

The ressources utilisation for the implementation of the AES-128 algorithm with the RIFFA framework on a Xilinx Virtex-6 ML605 development board are shown in Table I. For a clock rate of 250 Mhz, we achieved 391.25 Mbps

	Used	Available	Utilisation
Number of slice registers	7395	301440	2.4%
Number of slice LUTs	13146	150720	8.7%
Number of IOBs	10	600	1.6%
Number of block RAM/FIFO	34	52	65%
Clock rate	250 Mhz		
Throughput	391.25 Mbps		

TABLE I
RESSOURCES UTILISATION FOR THE IMPLEMENTATION OF THE AES ALGORITHM WITH THE RIFFA FRAMEWORK

VII. CONCLUSION

This paper introduced hardware acceleration of the AES cryptographicin the case of IPsec protocol. The modular structure that characterizes IPsec presents two main advantages. The first one is the offloading of the cryptographic computation from the software component to an FPGA accelerator through a PCIe bus. The second one is the ease of replacement of the encryption algorithm.

The present concept focuses on the AES encryption algorithm in ECB mode which constitutes the most consuming module in terms of computational resources of the IPsec protocol.

However, encryption algorithms are usually too complex for high-speed implementations, so the performance of the whole communication chain is usually limited by the encryption subsystem. To avoid overloading the central CPUs of the systems and speed up the communication systems, the security functions are more and more offloaded to FPGA network cards.

REFERENCES

[1] Pascal Paillier and Ingrid Verbauwhede . Multi-gigabit GCM-AES Architecture Optimized for FPGAs. In Cryptographic Hardware and Embedded Systems - CHES 2007, Pascal Paillier and Ingrid Verbauwhede. 2007. Springer Berlin Heidelberg, Berlin, Heidelberg.

[2] Mostafa I Soliman and Ghada Y Abozaid. 2011. FPGA implementation and performance evaluation of a high throughput crypto coprocessor. J. Parallel and Distrib. Comput. 71, 8 (2011), 1075–1084. https://doi.org/10.1016/j.jpdc.2011.04. 006.

[3] David Smekal, Jakub Frolka, and Jan Hajny. 2016. Acceleration of AES Encryption Algorithm Using Field Programmable Gate Arrays. IFAC-PapersOnLine 49, 25 (2016), 384 – 389. https://doi.org/10.1016/j.ifacol.2016.12.075 14th IFAC Conference on Programmable Devices and Embedded Systems PDES 2016.

[4] Yun Niu et al. 2013. An IPsec Accelerator Design for a 10Gbps Inline Security Network Processor. Institute of Microelectronics, Tsinghua University, Beijing, China.

[5] Joan Daemen and Vincent Rijmen. Specification for the Advanced Encryption Standard (AES). Federal Information Processing Standards Publication 197. 2001. http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf

[6] Matthew Jacobsen, Ryan Kastner. RIFFA 2.0: A Reusable Integration Framework for FPGA Accelerators. University of California, San Diago, USA. 2013

[7] Announcing the Advanced Encryption Standard (AES). Federal Information Processing Standards Publication 197. November 26, 2001.

Hand Biometry: A Review

Farah Bahmed[1,2]

1: Department of Computer Science
Ahmed Zabana University Centre, Relizane, 48000, Algeria
2: Signals and Images Laboratory
USTO-MB, BP 1505, El M'naouer, 31000, Oran, Algérie

farah.bahmed@univ-usto.dz (mostafarah@hotmail.fr)

Madani Ould Mammar[3,2]

3:Department of Electrical Engineering,
Faculty of Sciences and Technology

University Abdelhamid Ibn Badis, Mostaganem, Algeria

ouldmammar@univ-mosta.dz

***Abstract* - Using Hand to perform identity recognition is a very old technique adopted since thousands years. This paper presents an overview of different approaches concerning hand biometric systems developed in the literature. Focus is given on several modalities provided by the hand, and that can be used for personal recognition instead of the classical fingerprint. Multibiometric hand systems which combine two or more traits to increase recognition rate are also studied, and comparison of accuracy of different systems is provided.**

Index Terms* - *Biometry, Hand Recognition, Finger Recognition, Vein Recognition, Multimodality, Multibiometrics.

I. INTRODUCTION

Identity management using biometrics is more practical to use since it allows us to avoid the problem of stolen or forgotten passwords. Hand-based recognition systems offer many advantages as its good acceptance by users, its cheaper acquisitions devices and the huge amount of information it contains such as hand geometry, fingerprint, hand shape, finger vein, palmprint, palm vein, etc.

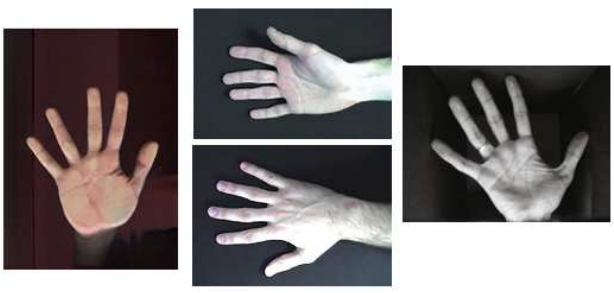
These security applications could be used as well as for access control as for contact-free payment [1][2]. In fact, hand which is very used nowadays by many systems for person recognition is a very old mean used since prehistoric era, when humans were signing their drawing with their handprint. Later, Babylonians also used to sign their commercial contracts with their handprint, as the Chinese did later also in the 7 th century. In 1858, Sir William Herschel used palmprints of Indian workers to manage the day of payment. In France, Alphonse Bertillon (1853-1914) who is known to be the developer of the judiciary anthropometry used palmprints, footprints and fingerprints to resolve criminal cases. The first automatic fingerprint recognition system was created in 1960, and in 1974 the first hand geometry system was designed. A hand geometry system was used in the 1996 Olympic Games for the access control to the Olympic Village, while Walt Disney World Park in Florida has also used for many years a finger geometry system to control entrance to the park and to avoid ticket fraud.

Nowadays, even laptops use fingerprint to secure access, and biometry systems using fingerprints and/or face are used in different airports of the world for passengers' control.

Hand systems can be categorized into two categories:

- Contact-based: The acquisition is performed either using pegs or similar guiding parts to force the user to put his/her hand in a certain manner, or using a flat surface, like a scanner.
- Contact-free: The acquisition is performed without any pegs or surface, the user has only to put his hand in front of a sensor. This sensor can be a digital camera, a webcam, a cell phone camera, etc.

It is bring to the attention of readers that some hand acquisition systems are known as "contact-free" while in fact they force the user to put his palmer or dorsal hand-side on a certain surface. Fig. 1 Illustrates samples of different public hand images databases.



(a) (b) (c)

Fig. 1. Samples of images from several databases; (a) Contact-based, (b) contact-free but with surface acquisition, (c) Contact-free without any surface acquisition

II. HAND RECOGNITION SYSTEMS

Firstly, there are two main phases in a biometric system:

1. Enrolment or registration: the image is first acquired from an authorized user, and then a preprocessing is applied, followed by a features extraction step, and finally, the storage of these features in a database of templates.
2. Recognition: image is acquired from a user then processed as the same way as for enrolment stage, except that at end features extracted are compared to those stored in the database.

Secondly, biometric system is composed of different steps which are:

A. Acquisition: image is acquired using a material device containing one or more sensors. In the case of hand, that sensor is usually a classical 2D visible light sensor, while some studies use an infrared sensor or combine the two sensors. Some other researches use instead a 3D acquisition device .

B. Preprocessing: hand is segmented and extracted from the background. This operation can be performed using region-based segmentation by an optimal

thresholding, or using contour-based segmentation by contour-based segmentation by contour detection and contour-fitting. Other operations can be performed in this step, like orientation correction of the hand.

C. Features extraction: from segmented hand (or only a part of it), algorithm performing features extraction is executed. In enrolment mode, these features are stored in the database as templates.
It must be highlighted that this step is generally preceded by keypoints detection step, to facilitate extraction of these characteristic features. Keypoints are generally fingers' tips and valleys.

D. Comparison: features extracted from current querying user are compared with templates stored in database to perform biometric recognition. This comparison is achieved using a simple distance or using a classifier.

Thus, biometric recognition can have two purposes:

A. Identification: consists to answer to the question:"Who is this person?". So, this operation implies a one-versus-N comparisons.
Based on comparison results, claimed identity is accepted or denied.

B. Authentication or verification: consists to answer to the question :"Is this person really who he/she claims to be?". So, this operation implies a one-versus-one comparison.
Based on comparison results, user is either accepted as a genuine user or rejected as imposter.

A great number of biometric systems have been proposed, so metrics to evaluate performance of each system must be defined. The performance of a biometric system can be measured by many standards metrics [3]:

- *FAR (False Accept Rate):* False acceptance is the number of times the system accepts an unauthorized user. It is the ratio of number of hands accepted incorrectly to the total number of hands out of database.
- *FRR (False Rejection Rate):* False rejection is the number of times the system rejects an authorized user. It is the ratio of number of hand images rejected to the total number of hands in database.
- *EER (Equal Error Rate or Cross over Error Rate):* The rates at which both accept and reject errors are equal. The value of the EER can be obtained from the FRR and FAR values with threshold graph.
- *CRR or TSR or CIR (Correct Recognition Ratio or True Success Rate or Correct Identification Rate):* It is defined as the ratio of number of hands correctly matched in the database to the total number of hands in the database.
- *DI (Discriminability Index):* Is the measurement of separability between genuine and imposter scores. It is defined as:

$$DI = \frac{|\mu_g - \mu_i|}{\sqrt{\frac{\sigma_g^2 + \sigma_i^2}{2}}} \quad (1)$$

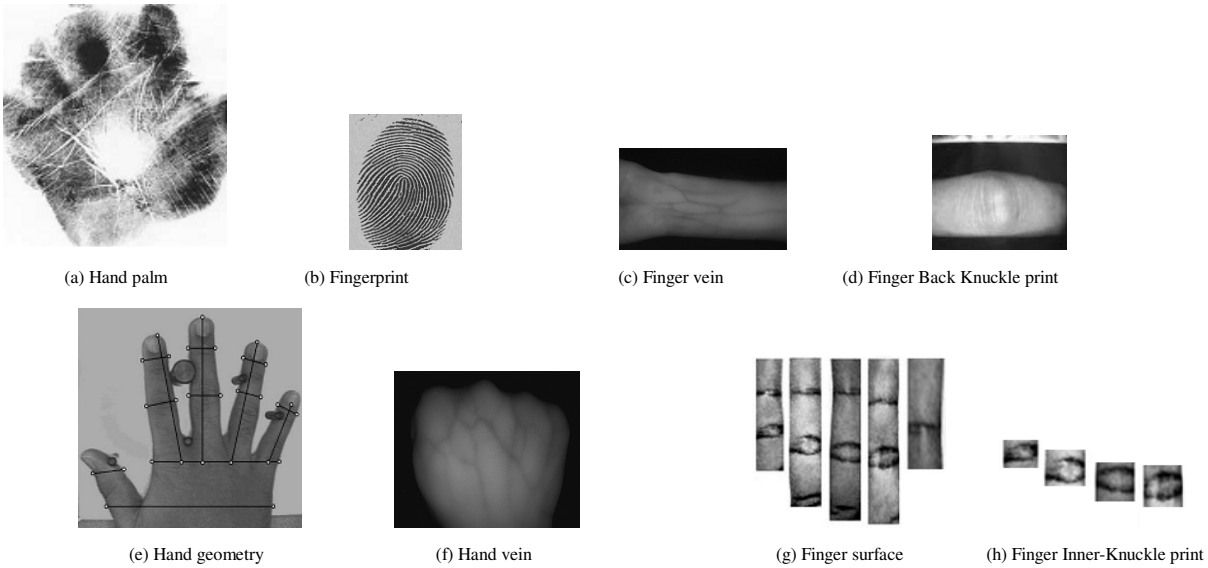
Where μ_g and μ_i are the means and σ_g and σ_i are the standard deviations of the genuine and imposter scores, respectively.
The system is efficient when the EER, FAR and FRR are minimum and when DI is maximum.

III. HAND MODALITIES

As seen in Section I, one of the main advantages of the hand is its wealth of informations which can be used as biometric trait. Fig. 2 Illustrates parts of the hand that can be used for biometric recognition purpose. Modalities used in the literature can be classed into four main groups:

- Geometry
- Contour (or shape)
- Surface (or texture)
- Vein

For each group, features can be extracted from the whole hand



(a) Hand palm (b) Fingerprint (c) Finger vein (d) Finger Back Knuckle print

(e) Hand geometry (f) Hand vein (g) Finger surface (h) Finger Inner-Knuckle print

Fig. 2 Different modalities provided by the hand

or only from a part. e.g., geometry features can be extracted from all the hand, i.e., fingers+palmprint, or only from fingers. Veins can be extracted from palm region or only from fingers, etc.

In next sections, a survey of different studies concerning each modality is presented. A survey of multibiometric hand systems is also proposed.

A. Geometry

This modality has been used commonly since 1970. Features describing hand geometry are generally fingers' widths, fingers' length, palm widths, fingers' area, etc. Each study proposes a set of features combined with a classification method. Some studies propose also a selection or reduction approach to decrease amount of features used. [4] have proposed a contact-free system which uses 34 hand geometry features. No evaluation of these features was performed. [5] have studied efficiency of geometry features. Genetic algorithm and Local Discriminant Analysis was used to reduce number of features from 400 to 50 on average. More recently, [6] have proposed a contact-based system which uses 62 features, and introduced new features like crookedness of fingers.

For performance accuracy, [6] have yielded an FAR=0% with an FRR= 1.19%, while [4] have showed an FAR=1.85% with a CIR=96.23%.

This modality presents the advantage of good acceptance by users, but the inconvenient of not being unique, since members of the same family can have very similar hand geometry characteristics.

B. Contour or shape

Consists to extract hand's contour features to perform biometric recognition. [7] have proposed a contact-based system which uses Hausdorff distance and Independant Components Analysis features. [8] have used high order Zernike moments to capture hand shape features. [9] have introduced a contact-based system using circular graph, which can be applied even in the case of non separated fingers, while for contact-free applications, [10] have proposed to use a new shape recognition method called Coherant Distance Shape Contexts, CDSC, to represent discriminative features from hand shape. [7] have showed a CIR=98.8%, while [10] have reached a very satisfactory EER of 0.9% using contour of four fingers.

It can be noted that this modality is not very used in the literature contrary to other modalities. Hand shape is more used for hand gesture recognition purpose than for biometric recognition purpose.

C. Surface or texture

Large dermal surface of the hand allows performing biometric recognition using many parts. Using palmprint surface was investigated a lot in literature as in [31] where wavelet decomposition is applied and in [32] where a 3D acquisition system is used. Palmprint offers the advantage of being a large surface than the fingerprint, with wrinkles and ridges.

Finger's texture was also studied, as in [11] where a CompCode method to encode finger's texture has been applied, and in [12] where and enhanced features extraction method called Enhanced Local Line Binary Pattern, *ELLBP*, was proposed to finger texture recognition. Another features extraction method was proposed by the same authors in [13].

To obtain smaller ROIs, some researches propose to use only a small area of the finger: the knuckle print. Thus, some researchers have studied accuracy of finger back knuckle print, FBKP, which is located in the dorsal side of the hand like [14] and [15], while other researches as [16] have studied using FIKP, which is located in the palmar side of the hand. Generally, studies work only on proximal knuckle or middle knuckle or major knuckle.

For accuracy rate, [32] have showed an EER= 1.39%, and [16] an EER= 3.65% in average for each finger.

So, hand surface is wealth of modalities useful for a biometric process, and it is the most technique used in the literature. The major drawback of using surface is the sensitivity to scars and cuts which modify epidermal appearance. Presence of dirt can also alter recognition efficiency.

D. Vein

Hand vein patterns are unique to everybody, even among identical twins, and cannot be affected by aging, cuts and scars. Vascular networks offer also more security than classical modalities such as fingerprint and palmprint, because veins are internal and cannot be falsified then. So, there is no way to cheat. [17] have proposed to use position corresponding relationship of endpoints and the intersection in the skeleton image. [18] have proposed to use relative distances and angles between a reference point and features points of the hand palmar vein.

Moreover, finger vein was also investigated in the literature as in [19] and in [20] where Adaptive Histogram Equalization enhancement was implemented.

Many of veins' systems reach an EER equal or lower to 1% using only palm vein, or only one or two fingers, what makes it a very powerful modality comparing to others, which need generally to combine informations from four or five fingers to achieve such accuracy. Veins offer also the advantage of not taking a capture of an external part of body, like a fingerprint, what makes it suitable to use. Contact-free payment systems use generally hand vein, since it require the user only to put his/her hand in front of the sensor. The inconvenient of such systems is that they require special infrared sensors which are expensive than classical visible light sensors.

IV. MULTIBIOMETRIC HAND SYSTEMS

Classical hand biometric systems, called unimodal systems, present in practice some limitations. The solution to overcome these limitations is generally multibiometrics. Multibiometrics combines use of several biometric sources to improve total accuracy. Each signal source is considered as a subsystem of the whole multibiometrics system [3]. There are six main kinds of multibiometrics systems:

- Multialgorithm systems: the same biometric trait is used for recognition but using different recognition

algorithms. E.g., fingerprint recognition from comparison of both minutiae and texture. Only one sensor is required for this kind of multibiometrics.

- Multisensors systems: the same biometric trait is captured using several sensors. E.g, fingerprint can be captured using both optical and compactive sensors.
- Multi-instance systems: the same biometric modality is captured several times. E.g, the capture of the thumb and the index of the same hand.
- Multisamples systems: is a variant of multi-instancesystems, where the same biometric trait has to be captured several times.
- Multimodal systems: combines different biometric modalities or characteristics to perform identity recognition.
- Hybrid systems: constituted of several of above-mentioned systems.

Fusion of data provided by different subsystems can be achieved at several levels:

- Sensor level: consists in fusion of captures to form a new capture.
- Feature level: consists in fusion of features sets of different subsystems.
- Score level: consists in fusion of scores provided by each subsystem.
- Decision level: each subsystem generates a decision according to its own score, and these decisions will be used to take a final decision.

Recently, many multibiometrics hand systems have been proposed in the literature. [21] have proposed a system which combines 24 finger geometry features and FBKP subspace features. [22] have introduced the possible use of minor (or distal or upper) FBKP in combination of major FBKP, using 1D Log-Gabor filter, and [23] have designed a system which makes use of minor FBKP and major FBKP with mean of Angular Geometric Analysis and Contourlet Transform. Combination use of FIKP, Finger geometry and palmprint was proposed in [24] with decision level fusion, while [25] have use combination of fingerprint, fingervein, and FIKP with a special acquisition device. Fusion was performed also at score level.

[26] have investigated the use of shape and 7 hand geometry features , with wavelet decomposition to reduce dimension of shape features, and bi-modal system was proposed in [27] that uses fusion of palmprint and hand shape.

An EER equal to 0% was reached by [28] who designed a special acquisition device which allows the use of 5 biometric modalities: Hand geometry, palmprint, palmvein, FIKP and finger vein.

[29] have proposed the use of major FIKP, minor FIKP and finger geometry for contact-free recognition. Size of geometry features was reduced using a statistical approach, and hierarchical fusion scheme has shown the best accuracy. Table I Summarizes a comparison of some state-of-art methods. As it can be seen, a large scale of systems are proposed by researchers, each one making use of a certain database for evaluation tests, and each one combining certain modalities using certain methods. High accuracy is reached by multibiometrics systems with error rate equals to 0% or almost equals 0%, comparing with unimodal systems.

TABLE I. COMPARISON OF SOME STATE-OF-ART METHODS

Reference (year)	Biometric modalities	Number of subject	Peg-free?	Surface used?	Results
[30] (2007)	HG +PP+FP+FIKP	200	No		EER=0.0005%
[21] (2009)	FG + Major FBKP	105	Yes	Yes	EER=1.39%
[24](2010)	FIKP+FG+PP	190	Yes	Yes	FRR=0.898% FAR=2.52 e^{-6}
[22] (2012)	Major FBKP+ Minor FBKP	202	Yes	Yes	EER=0.16%
[28] (2012)	HG+PP+PV+FIKP+FV	136	Yes	No	EER=0.00%
[25] (2015)	FP+ Major FIKP+FV	378	No		EER=0.109%
[26] (2015)	HG+ HS	50 (JUET) 240 (IITD)	No Yes	 No	EER=0.31% EER=0.52%
[23] (2016)	Major FBKP+ Minor FBKP+FG	150	Yes	Yes	EER=0.44%
[27](2018)	HS+PP	139	Yes	No	EER=7%
[29] (2019)	Major FIKP + Minor FIKP+ FG	100 (IITD)	Yes	No	FRR=0% FAR=0.12%

PP=Palmprint PV=Palm Vein FIKP= Inner Knuckle Print FG=Finger Geometry

FBKP=Finger Back Knuckle Print HG=Hand Geometry FV= Finger Vein HS=Hand Shape

V. CONCLUSION

The aim of this work was to give a succinct overview of different techniques of hand biometry. Several modalities were presented and studies using these modalities were introduced. Multibiometrics systems that combine two or more modalities were also investigated and a comparison between state of art methods was exposed. Analysis of these systems confirms their accuracy in comparison of classical unimodal systems.

We can say that hand is really a very useful identity management mean, and considerable progress has been made in this field of research, and it should take more part in world biometry market in the future.

REFERENCES

[1] Quixter: Biometric payment system of Sweden. https://www.youtube.com/watch?v=qilvq52nnQ0. Last accessed on 13 th may 2019

[2] https://keyo.co/ . Last accessed on 13 th may 2019

[3] A. Naït-Ali and R. Fournier, Signal and Image Processing for Biometrics. ISTE Ltd and John Wiley & Sons, Inc. 2012.

[4] J. M. Guo, C. H. Hsia, Y. F. Liu, J. C. Yu, M. H. Chu and T. N. Le, "Contact-free hand geometry-based identification system", Expert Systems with Applications 39 (2012) 11728–11736.

[5] R. M. Luque-Baena, D. Elizondo, E. López-Rubio, E. J. Palomo and T. Watson, "Assessment of geometric features for individual identification and verification in biometric hand systems", Expert Systems with Applications 40 (2013) 3580–3594.

[6] M. Klonowski, M. Plata, P. Syga, "User authorization based on hand geometry without special equipment", Pattern Recognition 73 (2018) 189–201. http://dx.doi.org/10.1016/j.patcog.2017.08.017

[7] E. Yörük, E. Konukolu, B. Sankur and J. Darbon, "Shape Based Hand Recognition", IEEE TRANSACTIONS ON IMAGE PROCESSING, VOL. 15, NO. 7, JULY 2006.

[8] G. Amayeh, G. Bebis, A. Erol, and M. Nicolescu, "Peg-Free Hand Shape Verification Using High Order Zernike Moments", Computer Vision and Pattern Recognition Workshop, 2006 Conference on. DOI: 10.1109/CVPRW.2006.155

[9] I. Bakina L. Mestetskiy, "Hand Shape Recognition from Natural Hand Position". 978-1-4577-0490-1/11.

[10] R.-X. Hu, W. Jia, D. Zhang, J. Gui and L.-T. Song, "Hand shape recognition based on coherent distance shape contexts", Pattern Recognition 45 (2012) 3348–3359

[11] V. Kanhangad, A. Kumar and D. Zhang, "A unified framework for contactless hand verification", IEEE Trans. Inf. Forensics Secur. 6(3) (2011) 1014–1027.

[12] R.R.O. Al-Nima, S.S. Dlay, S.A.M. Al-Sumaidaee, W.L. Woo and J.A. Chambers, "Robust feature extraction and salvage schemes for finger texture based biometrics", IET Biometrics 6(2) (2016) 43–52, http://dx.doi.org/10.1049/iet-bmt.2016.0090

[13] R.R.O. Al-Nima, M.A.M. Abdullah, M.T.S. Al-Kaltakchi, S.S. Dlay, W.L. Woo and J.A. Chambers, "Finger texture biometric verification exploiting Multi-scale Sobel Angles Local Binary Pattern features and score-based fusion", Digital Signal Processing 70 (2017) 178–189. http://dx.doi.org/10.1016/j.dsp.2017.08.002

[14] L. Zhang, L. Zhang, D. Zhang and H. Zhu, "Online Finger-Knuckle-Print Verification for Personal Authentication ".

[15] L. Zhang, L. Zhang and D. Zhang, "FINGER-KNUCKLE-PRINT: A NEW BIOMETRIC IDENTIFIER", 2009, 16th IEEE International Conference on Image Processing (ICIP). DOI: 10.1109/ICIP.2009.5413734

[16] M. Liu, Y. Tian and L. Li, "A new approach for inner-knuckle-print recognition". Journal of Visual Languages and Computing 25, 33–42. doi:10.1016/j.jvlc.2013.10.003

[17] L. Xirong, Z. Bo, S. Xiaosheng, Z. Yunlong and B. Guiqiu, "Measurement and matching of human vein pattern characteristics", 43(2), 164-167. 2003.

[18] Y.-P. Hu, Z.-y. Wang, X.-p. Yang and Y.-m. Xu, "Hand vein recognition based on the connection lines of reference point and feature point", Infrared Physics & Technology 62 (2014) 110–114. http://dx.doi.org/10.1016/j.infrared.2013.10.004

[19] H. Qin, X. He, X. Yao and H. Li, "Finger-vein verification based on the curvature in Radon space", Expert Syst. Appl. 2017, 82, 151–161.

[20] J. Yang, Y. Shi, G. Jia, "Finger-vein image matching based on adaptive curve transformation", Pattern Recognit. 2017, 66, 34–43.

[21] A. Kumar and C. h. Ravikanth, "Personal authentication using finger knuckle surface". IEEE Transactions on Information Forensics and Security, 4(1), pp. 98–110. 2009. doi:10.1109/TIFS.2008.2011089.

[22] A. Kumar, "Can we use minor finger knuckle images to identify humans?", IEEE Fifth International Conference on Biometrics. 2012. doi:10.1109/BTAS.2012.6374558.

[23] K. Usha and M. Ezhilarasan, "Fusion of geometric and texture features for finger knuckle surface recognition", Alexandria Engineerng Journal, 55, 683–697. 2016. doi:10.1016/ j.aej.2015.10.003

[24] L. Q. Zhu and S. Y. Zhang, "Multimodal biometric identification system based on finger geometry, knuckle print and palm print". Pattern Recognition Letters 31(2010), 1641–1649. 2010. doi:10.1016/j.patrec.2010.05.010

[25] W. Kang, X. Chen and Q. Wu, "The biometric recognition on contactless multi-spectrum finger images", Infrared Physics and Technology, 68, 19–27. 2015. doi:10.1016/j.infrared.2014.10.007

[26] S. Sharma, S. R. Dubey, S. K. Singh, R. Saxena and R. K. Singh, "Identity verification using shape and geometry of human hands", Expert Systems with Applications, 42, 821–832. 2015. doi:10.1016/j.eswa.2014.08.052.

[27] W-S. Chen and W-C. Wang, "Fusion of hand-shape and palm-print traits using morphology for bi-modal biometric authentication", Int. J. Biometrics, Vol. 10, No. 4, pp.368–390. 2018.

[28] G. K. O. Michael, T. Connie & A. B. J. Teoh, "A contactless biometric system using multiple hand features", Journal of Visual Communication and Image Representation. 23(7), 1068–1084. 2012. doi:10.1016/j.jvcir.2012.07.004

[29] F. Bahmed, M. Ould Mammar and A. Ouamri, "A Multimodal Hand Recognition System Based on Finger Inner-Knuckle Print and Finger Geometry", Journal of Applied Security Research, 2019. DOI:10.1080/19361610.2019.1545271

[30] T. Savic and N. Pavešic, "Personal recognition based on an image of the palmar surface of the hand", Pattern Recognition, 40, 3152–3163. doi:10.1016/j.patcog.2007.03.005.

[31] S.M. Prasad, V.K. Govindan and P.S. Sathidevi, "Palmprint Authentication Using Fusion of Wavelet Based Representation", 978-1-4244-5612-3/09, 2009. IEEE.

[32] B. Zhang, W. Li, P. Qing and D. Zhang, "Palm-Print Classification by Global Features", IEEE TRANSACTIONS ON SYSTEMS,MAN, AND CYBERNETICS: SYSTEMS, VOL. 43, NO. 2,MARCH 2013. DOI: 10.1109/TSMCA.2012.2201465

Implementation and statistical tests of a block cipher algorithm MISTY1*

1st Moussaoui Sarah
Laboratoire Centrale de R&D
ECRMT
Algiers, Algeria
moussaouisarah1105@gmail.com

2nd Zeghdoud Sabrina
Laboratoire de Recherche en Electonique et Ingénieurie des Systèmes Electroniques
AMC
Algiers, Algeria
sabrinazeghdoud5@gmail.com

3rd Allailou Boufeldja
Institue de Recherche et Developpement
ESCH
Algiers, Algeria
boufeldja.allailou@gmail.com

***Abstract*—With the development of communication network and new information technologies, the volume of data exchanged is growing, particularly with the of IoTs. There security has become a major concern, specially in sensitive activities. Such security requirements call for efficient cryptographic encryption algorithms, with a small hardware footprint. The current trend is towards light cryptographic algorithms (lightwieght). These are designed for power systems with limited storage capacity. This paper proposes the study, hardware implementation and statistical test of block cipher algorithm MISTY1. Its optimized version for a hardware implementation is known as KASUMI, used in the context of 3GPP compliant mobile networks, including 2G (GSM) and 3G (UMTS).**

***Index Terms*—Cryptography, Block cipher, MISTY1, KASUMI, Hardware Implementation, FPGA, NIST statistical test.**

I. Introduction

MISTY1 (*Mitsubishi Improved Security Technology*) is a 64-bit block cipher with a 128-bit secret key, and a variable number of rounds, based on a Feistel scheme. Its detailed description and specifications were first published in Japan in 1996 [5] before being presented at "*The international workshop of Fast Software Encryption* "in 1997 [6].

Its optimized version for a hardware implementation is known as KASUMI [1], used in the context of 3GPP compliant mobile networks, including 2G (GSM) and 3G (UMTS). As a result, KASUMI and MISTY1 are very similar, "KASUMI" is also the Japanese translation of the word "MISTY" (foggy).

In this paper, we describe the *MISTY1* algorithm, the encryption-decryption procedure, the key management process and the component functions.

We suggest a practical application which consists in the implementation of the *MISTY1* algorithm on *FPGA* map, using *VHDL* programming language.

In this context, we propose a purely combinatorial implementation approach. The algorithmic programming of the suggested approach is based on the subdivision of the structure of the *MISTY1* algorithm into three essential parts, namely, the key management process, the management of the encryption sub-keys and the encryption-decryption procedure itself.

Behavioral simulations under *ISIM* were performed to validate the implemented program. Subsequently, a hardware check on the *FPGA* card, through the integrated logic analyzer *Chipscope Pro*, was also performed.

This paper is organized as follows: in the first section, we present the algorithm in question as well as the different equations that compose it. In the second section, we present the adopted implementation approach, the simulations under *ISIM* of the designed program of the *MISTY1* algorithm. In the next section, we show a hardware check on map *FPGA*. Then, we will present the execution results of the algorithm taken from the integrated logic analyzer (*ChipScope*). Finally, we will present the NIST statiscal results.

II. Description of MISTY1

MISTY1 is a Fiestel block cipher with a 64-bits block and a 128-bits key. It is among the final NESSIE portfolio of block ciphers [3], and has been recommanded for Japanese e-Government cipher by the CRYPTREC project [2].

A. MISTY1 Structure

1) Encryption Process: Fig 1 presents *MISTY1* encrypting procedure for n tours. The plaintext of 64 bits ($P_{(64)}$) is divided into two parts, 32 bits on the left and 32 on the right, which will be transformed into a 64-bit encrypted text ($C_{(64)}$) by means of exclusive-OR logic operations (Xor), FO_i functions ($1 \leq i \leq n$) and FL_i ($1 \leq i \leq n+2$) functions [4]. The FO_i function uses two sub-keys, one of 64 bits (KO_i) and another of 48 bits (KI_i). The FL_i function uses a 32-bit sub-key (KL_i). Subkeys used during the encryption process are generated from the main secret key ($K_{(128)}$)

In the encryption process, the first step is to divide the 64-bit plaintext ($P_{(64)}$) into two 32-bit length parts, ie $P(64) = L_{0(32)} \parallel R_{0(32)}$. Then the following operations are performed:

For odd rounds ($i = 1, 3, ..., n-1$), we define:

$$R_i = FL_i(L_{i-1}, KL_i) \tag{1}$$

$$L_i = FL_{i+1}(R_{i-1}, KL_{i+1}) \oplus FO_i(R_i, KO_i, KI_i) \tag{2}$$

For pair rounds ($i = 2, 4, ..., n$), we define: :

$$R_i = L_{i-1} \tag{3}$$

$$L_i = R_{i-1} \oplus FO_i(R_i, KO_i, KI_i) \tag{4}$$

After the last round ($n = 8$), the FL function is applied to the two data L_n and R_n, to get:

$$R_{n+1} = FL_{n+1}(L_n, KL_{n+1}) \tag{5}$$

$$L_{n+1} = FL_{n+2}(R_n, KL_{n+2}) \tag{6}$$

The concatenation of the two resulting data $L_{n+1(32)}$ and $R_{n+1(32)}$ forms the ciphertext output.

$$C_{(64)} = L_{n+1(32)} \parallel R_{n+1(32)} \tag{7}$$

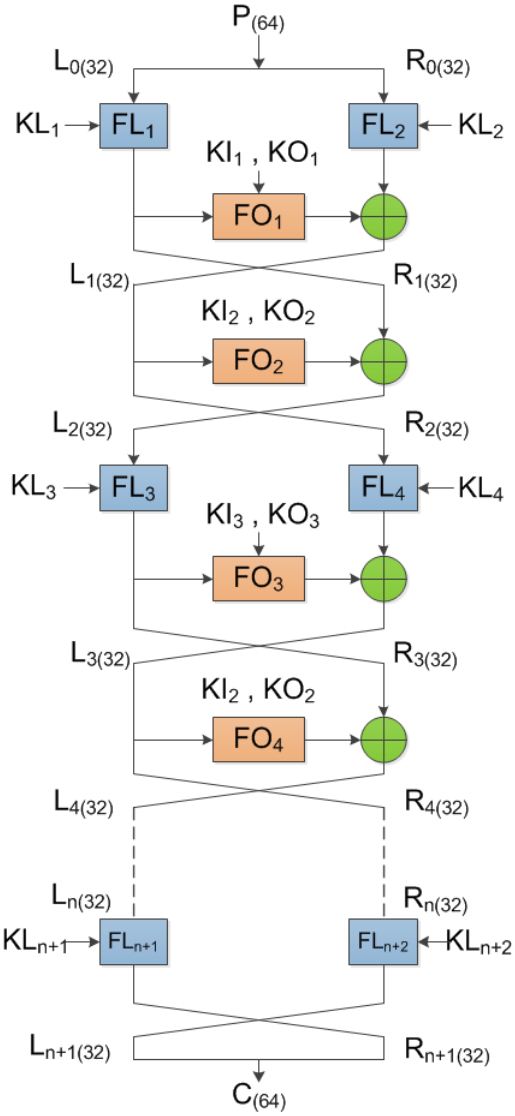


Fig. 1. MISTY1 encryption process.

2) Decryption Process: MISTY1 decryption procedure is done in the same way as the encryption process, by inverting the order of the sub-keys and replacing the function FL by the function FL^{-1} [4]. Fig 2 illustrates the decryption process of the algorithm MISTY1 with n rounds [4].

The 64-bit encrypted text ($C_{(64)}$ is split into two 32-bit parts, and will be transformed into a 64-bit plaintext ($P_{(64)}$)

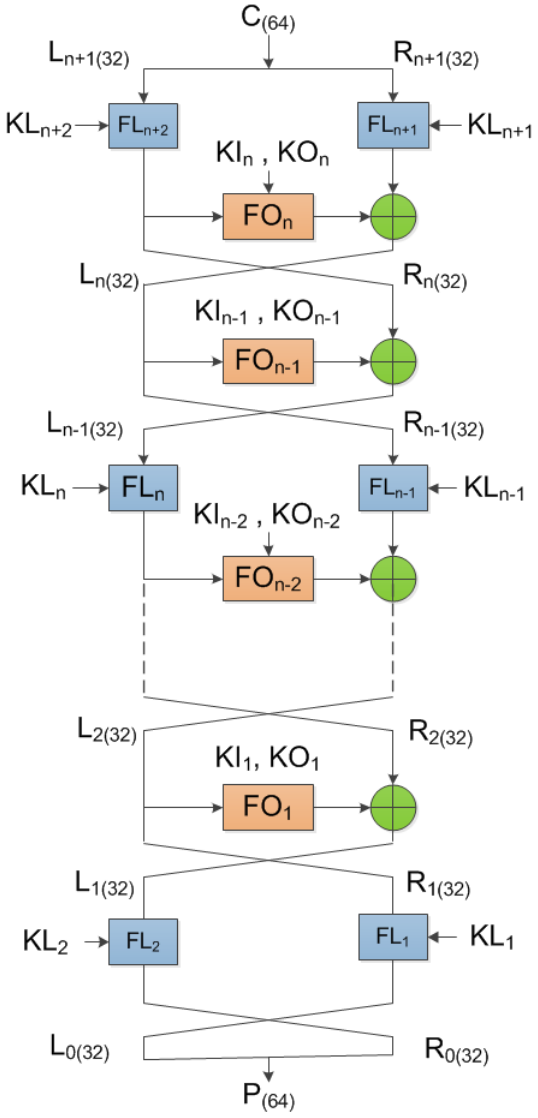


Fig. 2. MISTY1 decryption process.

using the logical operation Xor and the two subfunctions FO_i ($n \leq i \leq 1$) and FL_i^{-1} ($n + 2 \leq i \leq 1$).

During the decryption process, the ciphertext ($C_{(64)}$) is divided into two 32-bit length parts ($C_{(64)} = L_{n+1(32)} \parallel R_{n+1(32)}$), and will undergo the operations below:

For odd rounds ($i = n - 1, ..., 3.1$), we define:

$$R_i = FL_{i+2}^{-1}(L_{i+1}, KI_{i+2}) \tag{8}$$

$$L_i = FL_{i+1}^{-1}(R_{i+1}, KL_{i+1}) \oplus FO_i(R_i, KO_i, KI_i) \tag{9}$$

For pair rounds ($i = n, ..., 4, 2$), we define :

$$R_i = L_{i+1} \tag{10}$$

$$L_i = R_{i+1} \oplus FO_i(R_i, KO_i, KI_i) \tag{11}$$

After the n^{th} round ($n = 8$), the FL^{-1} function is applied to the data L_1 and R_1, as follows:

$$R_0 = FL_2^{-1}(L_1, KL_2) \tag{12}$$

$$L_0 = FL_1^{-1}(R_1, KL_1) \tag{13}$$

Finally, the two data L_0 and R_0 are concatenated to give as output the plaintext $P_{(64)}$.

$$P_{(64)} = L_{0(32)} \parallel R_{0(32)} \tag{14}$$

3) Encrypion key management: MISTY1 uses a 128-bit secret key ($K_{(128)}$), subdivided into eight sub-keys of 16 bits $(K_{1(16)}), K_{2(16)}, ..., K_{8(16)})$ as follows

$$K_{(128)} = K_{1(16)} \parallel K_{2(16)} \parallel K_{3(16)} \parallel K_{4(16)} \parallel K_{5(16)} \parallel K_{6(16)} \parallel K_{7(16)} \parallel K_{8(16)}. \tag{15}$$

The key management procedure yields a 128-bit sub-key $(K'_{(128)})$, formed by concatenating eight 16-bit words [4] $(K'_{1(16)}), K'_{2(16)}), ..., K'_{8(16)}))$. Figure 3 shows the key management procedure.

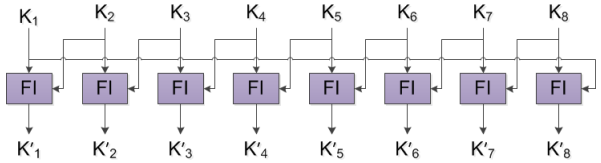


Fig. 3. Key Management Scheme.

The K'_i $(1 \leq i \leq 7)$ are deduced from the following equation:

$$K_i{}'_{(16)} = FI(K_{i(16)}, K_{i+1(16)}) \tag{16}$$

for $i = 8, K_8{}'_{(16)} = FI(K_{8(16)}, K_{1(16)})$.

The correspondence between the sub-keys $KO_{ij}, KI_{ij}, KL_{ij}$ used during the i^{th} round and the sub-keys K_i, K'_i is given in the table I.

KO_{i1}	KO_{i2}	KO_{i3}	KO_{i4}	KI_{i1}	KI_{i2}	KI_{i3}	KL_{iL}	KL_{iR}
K_i	K_{i+2}	K_{i+7}	K_{i+4}	K'_{i+5}	K'_{i+1}	K'_{i3}	$K_{\frac{i+1}{2}}$ (i odd) $K'_{\frac{i}{2}+2}$ (i pair)	$K'_{\frac{i+1}{2}+6}$ (i odd) $K_{\frac{i}{2}+4}$ (i pair)

TABLE I
ENCRYPTION SUBKEYS MANAGEMENT

B. Components of MISTY1

1) FL function: Figure 4 represents the logic diagram of the FL function, which uses 32-bit input data $(X_{(32)})$ and a 32-bit sub-key $(KL_{i(32)})$ are used [4]. The input data $X_{(32)}$ is divided into two 16-bit words ($X_{L(16)}$ and $X_{R(16)}$), where:

$$X_{(32)} = X_{L(16)} \parallel X_{R(16)} \tag{17}$$

The sub-key $KL_{i(32)}$ is divided into two sub-keys of 16 bits, $KL_{iL(16)}$ and $KL_{iR(16)}$, where:

$$KL_{i(32)} = KL_{iL(16)} \parallel KL_{iR(16)} \tag{18}$$

We define :

$$Y_{R(16)} = (X_{L(16)} \cap KL_{iL(16)}) \oplus X_{R(16)} \tag{19}$$

$$Y_{L(16)} = (Y_{R(16)} \cup KL_{iR(16)}) \oplus X_{L(16)} \tag{20}$$

The FL function outputs 32-bit data $(Y_{(32)})$, defined as follows:

$$Y_{(32)} = Y_{L(16)} \parallel Y_{R(16)} \tag{21}$$

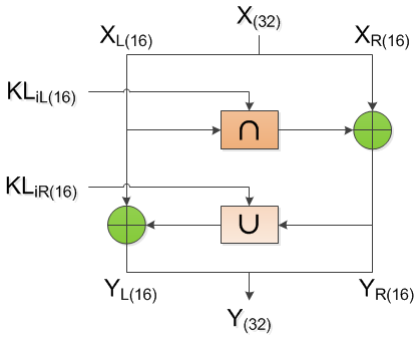


Fig. 4. FL function.

2) $FL^{-1}function$: Figure 5 represents the logical scheme of the function FL^{-1}. The FL^{-1} function uses a 32-bit input $(Y_{(32)})$ and a 32-bit sub-key $(KL_{i(32)})$ [4].

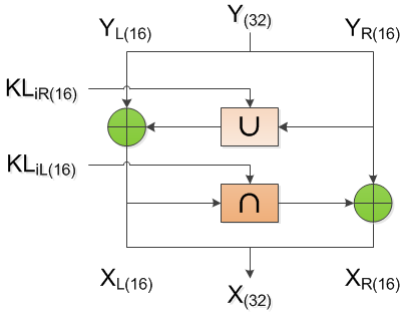


Fig. 5. FL^{-1} function.

The input data $Y_{(32)}$ is divided into two 16-bit words ($Y_{L(16)}$ and $Y_{R(16)}$), where:

$$Y_{(32)} = Y_{L(16)} \parallel Y_{R(16)} \tag{22}$$

The sub-key $KL_{i(32)}$ is divided into two sub-keys of 16 bits, $KL_{iL(16)}$ and $KL_{iR(16)}$, where:

$$KL_{i(32)} = KL_{iL(16)} \parallel KL_{iR(16)} \tag{23}$$

We define :

$$X_{R(16)} = (Y_{R(16)} \cup KL_{iR(16)}) \oplus Y_{L(16)} \tag{24}$$

$$X_{R(16)} = (X_{L(16)} \cap KL_{iL(16)}) \oplus Y_{R(16)} \tag{25}$$

The FL^{-1} function outputs 32-bit data ($Y_{(32)}$), are defined as follows:

$$X_{(32)} = X_{L(16)} \parallel X_{R(16)} \tag{26}$$

3) FO function: The FO function uses 32-bit input data ($Y_{(32)}$) and two sub-keys, one of 64 bits ($KO_{i(64)}$) and another of 48 bits [4]. The logic diagram of the FO function is shown in fig 6.

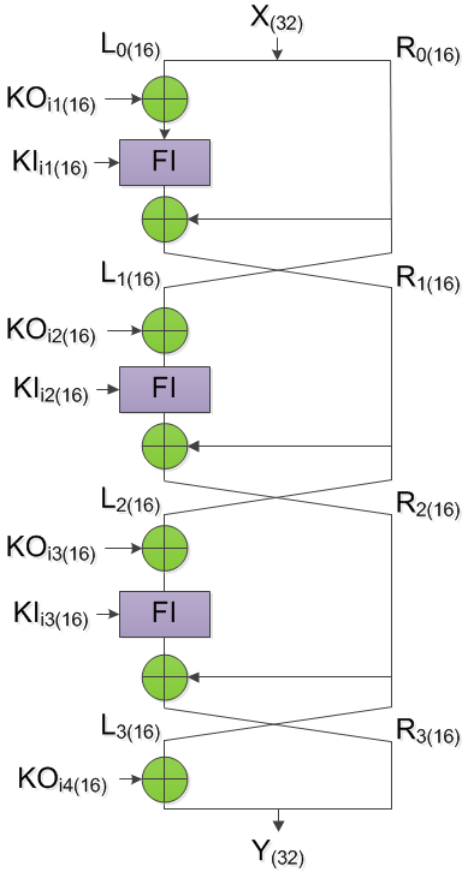


Fig. 6. FO function.

The input data $X_{(32)}$ is divided into two half-words (16-bits) ($L_{0(16)}, R_{0(16)}$), where:

$$X_{(32)} = L_{0(16)} \parallel R_{0(16)} \tag{27}$$

The two sub-keys are divided into 16-bit sub-keys:

$$KO_{i(64)} = KO_{i1(16)} \parallel KO_{i2(16)} \parallel KO_{i3(16)} \parallel KO_{i4(16)}. \tag{28}$$

$$KI_{i(48)} = KI_{i1(16)} \parallel KI_{i2(16)} \parallel KI_{i3(16)}. \tag{29}$$

For an integer j, with (1 $leqj$ leq3) we define:

$$R_j = FI_{ij}(Lj - 1 \oplus KO_{ij}, KI_{ij}) \oplus R_{j-1} \tag{30}$$

$$L_j = R_{j-1} \tag{31}$$

Finally, the FO function outputs 32-bit data ($Y_{i(32)}$), is defined as follows:

$$Y_{i(32)} = (L_{3(16)} \oplus KO_{i4}) \parallel R_{3(16)} \tag{32}$$

4) FI fonction : The function FI_j has a 16-bit word ($X_{j(16)}$ for data input and uses a 16-bit sub-key ($KI_{ij(16)}$) [4]. The input data and the sub-key are each divided into two words of different lengths ($L_{0(9)}$ and $R_{0(7)}$) and ($KI_{ijL(7)}$ and $KI_{ijR(9)}$). With:

$$X_{j(16)} = L_{0(9)} \parallel R_{0(7)} \tag{33}$$

$$KI_{ij(16)} = KI_{ijL(7)} \parallel KI_{ijR(9)} \tag{34}$$

The FI function uses two S-Boxes, S7 which links a 7-bit input to a 7-bit output, and S9 which links a 9-bit input to a 9-bit output [4]. In addition, it uses two additional functions designated by ZE and TR, (fig 7), defined as:

- The ZE function converts a 7-bit value ($x_{(7)}$) into a 9-bit value ($y_{(9)}$) by adding two null bits to the left of the most significant bit ($y_{(9)} = ZE(x_{(7)})$).
- The function TR converts a value of 9 bits ($x_{(9)}$) into a value of 7 bits ($y_{(9)}$) by eliminating the two most significant bits ($y_{(7)} = TR(x_{(9)})$).

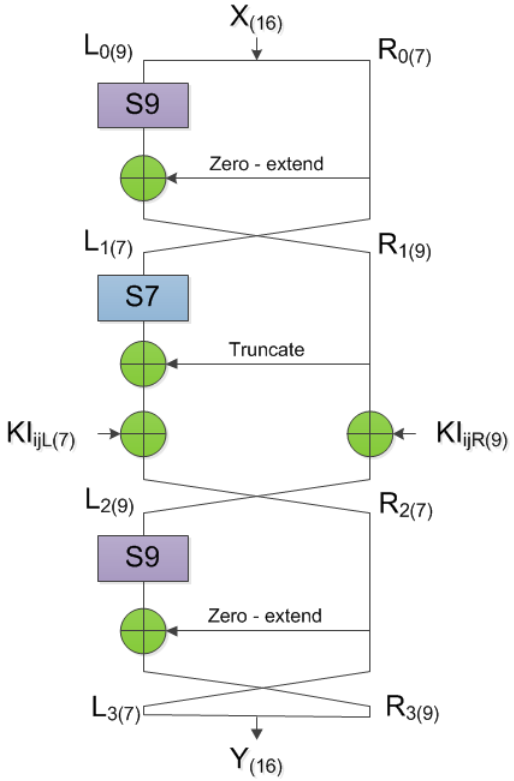


Fig. 7. FI function.

The output data ($Y_{(16)}$) is given by:

$$Y_{(16)} = L_{3(7)} \parallel R_{3(9)} \tag{35}$$

The values $L_{3(7)}$ and $R_{3(9)}$ are obtained after the following series of operations:

$$L_{1(7)} = R_{0(7)} \tag{36}$$

$$R_{1(9)} = S9(L_{0(9)}) \oplus ZE(R_{0(7)}) \tag{37}$$

$$L_{2(9)} = R_{1(9)} \oplus KI_{ijR(9)} \quad (38)$$

$$R_{2(7)} = S7(L_{1(7)}) \oplus TR(R_{1(9)}) \oplus KI_{ijL(7)} \quad (39)$$

$$L_{3(7)} = R_{2(7)} \quad (40)$$

$$R_{3(9)} = S9(L_{2(9)}) \oplus ZE(R_{2(7)}) \quad (41)$$

5) S-Boxes: The two S-Boxes are designed in a simple hardware or software implementation, as well as in combinatorial logic or by using a look-up table [4]. What follows will summarize the analytical equations describing the two S-Boxes:

- The logical equations describing S-Boxing S7:

$y_0 = x_0 \oplus x_1x_3 \oplus x_0x_3x_4 \oplus x_1x_5 \oplus x_0x_2x_5 \oplus x_4x_5 \oplus x_0x_1x_6 \oplus x_2x_6 \oplus x_0x_5x_6 \oplus x_3x_5x_6 \oplus 1$
$y_1 = x_0x_2 \oplus x_0x_4 \oplus x_3x_4 \oplus x_1x_5 \oplus x_2x_4x_5 \oplus x_6 \oplus x_0x_6 \oplus x_3x_6 \oplus x_2x_3x_6 \oplus x_1x_4x_6 \oplus x_0x_5x_6 \oplus 1$
$y_2 = x_1x_2 \oplus x_0x_2x_3 \oplus x_4 \oplus x_1x_4 \oplus x_0x_1x_4 \oplus x_0x_5 \oplus x_0x_4x_5 \oplus x_3x_4x_5 \oplus x_1x_6x_3x_6 \oplus x_0x_3x_6 \oplus x_4x_6 \oplus x_2x_4x_6$
$y_3 = x_0 \oplus x_1 \oplus x_0x_1x_2 \oplus x_0x_3 \oplus x_2x_4 \oplus x_1x_4x_5 \oplus x_2x_6 \oplus x_1x_3x_6 \oplus x_0x_4x_6 \oplus x_5x_6 \oplus 1$
$y_4 = x_2x_3 \oplus x_0x_4 \oplus x_1x_3x_4 \oplus x_5 \oplus x_2x_5 \oplus x_1x_2x_5 \oplus x_0x_3x_5 \oplus x_1x_6 \oplus x_1x_5x_6 \oplus x_4x_5x_6 \oplus 1$
$y_5 = x_0 \oplus x_1 \oplus x_2 \oplus x_0x_1x_2 \oplus x_0x_3 \oplus x_1x_2x_3 \oplus x_1x_4 \oplus x_0x_2x_4 \oplus x_0x_5 \oplus x_0x_1x_5 \oplus x_3x_5 \oplus x_0x_6 \oplus x_2x_5x_6$
$y_6 = x_0x_1 \oplus x_3 \oplus x_0x_3 \oplus x_2x_3x_4 \oplus x_0x_5 \oplus x_2x_5 \oplus x_3x_5 \oplus x_1x_3x_5 \oplus x_1x_6 \oplus x_1x_2x_6 \oplus x_0x_3x_6 \oplus x_4x_6 \oplus x_2x_5x_6$

-The logical equations describing S-Boxing S9:

$y_0 = x_0x_4 \oplus x_0x_5 \oplus x_1x_5 \oplus x_1x_6 \oplus x_2x_6 \oplus x_2x_7 \oplus x_3x_7 \oplus x_3x_8 \oplus x_4x_8 \oplus 1$
$y_1 = x_0x_2 \oplus x_3 \oplus x_1x_3 \oplus x_2x_3 \oplus x_3x_4 \oplus x_4x_5 \oplus x_0x_6 \oplus x_2x_6 \oplus x_7 \oplus x_0x_8 \oplus x_3x_8 \oplus x_5x_8 \oplus 1$
$y_2 = x_0x_1 \oplus x_1x_3 \oplus x_4 \oplus x_0x_4 \oplus x_2x_4 \oplus x_3x_4 \oplus x_4x_5 \oplus x_0x_6 \oplus x_5x_6 \oplus x_1x_7 \oplus x_3x_7 \oplus x_8$
$y_3 = x_0 \oplus x_1x_2 \oplus x_2x_4 \oplus x_5 \oplus x_1x_5 \oplus x_3x_5 \oplus x_4x_5 \oplus x_5x_6 \oplus x_1x_7 \oplus x_6x_7 \oplus x_2x_8 \oplus x_4x_8$
$y_4 = x_1 \oplus x_0x_3 \oplus x_2x_3 \oplus x_0x_5 \oplus x_3x_5 \oplus x_6 \oplus x_2x_6 \oplus x_4x_6 \oplus x_5x_6 \oplus x_6x_7 \oplus x_2x_8 \oplus x_7x_8$
$y_5 = x_2 \oplus x_0x_3 \oplus x_1x_4 \oplus x_3x_4 \oplus x_1x_6 \oplus x_4x_6 \oplus x_7 \oplus x_3x_7 \oplus x_5x_7 \oplus x_6x_7 \oplus x_0x_8 \oplus x_7x_8$
$y_6 = x_0x_1 \oplus x_3 \oplus x_1x_4 \oplus x_2x_5 \oplus x_4x_5 \oplus x_2x_7 \oplus x_5x_7 \oplus x_8 \oplus x_0x_8 \oplus x_4x_8 \oplus x_6x_8 \oplus x_7x_8 \oplus 1$
$y_7 = x_1 \oplus x_0x_1 \oplus x_1x_2 \oplus x_2x_3 \oplus x_0x_4 \oplus x_5 \oplus x_1x_6 \oplus x_3x_6 \oplus x_0x_7 \oplus x_4x_7 \oplus x_6x_7 \oplus x_1x_8 \oplus 1$
$y_8 = x_0 \oplus x_0x_1 \oplus x_1x_2 \oplus x_4 \oplus x_0x_5 \oplus x_2x_5 \oplus x_3x_6 \oplus x_5x_6 \oplus x_0x_7 \oplus x_0x_8 \oplus x_3x_8 \oplus x_6x_8 \oplus 1$

III. Hardware implementation

A. Implementation approach

In this section, we present *MISTY1* programming approach , using the *VHDL* language, starting from the previousely studied description.

The first block is responsible for the process of managing the secret key. Starting from the secret key K with a length of 128 bits, we have a sub-key K' of 128 bits. the detailed description of the process has been given in section II-A3. Keys K and K' are used as input data for the second logical block (management block of encryption sub-keys (Figure 8)). This block will provide the encryption sub-keys KO_{ij}, KI_{ij} and KL_i.Figure 8 illustrates the architecture of the *MISTY1* algorithm as described in *VHDL*.

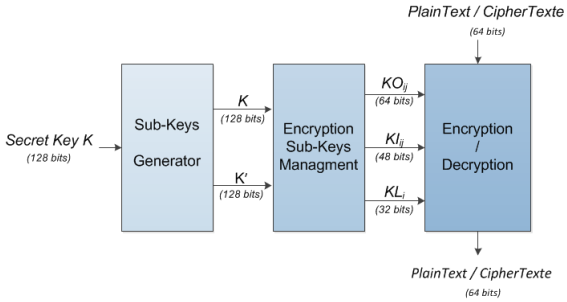


Fig. 8. Structure of the implementation program of the algorithm MISTY1

The last block ensures the execution of the 64-bit block encryption-decryption procedure. It is designed from the description given by the fig **??**. The algorithmic of the program is totally inspired by the figure.

Data	**Value** (in hexadecimal)
Secret key (K_1 à K_8) (128 bits)	00 11 22 33 44 55 66 77 88 99 aa bb cc dd ee ff
Sub-key (K'_1 à K'_8) (128 bits)	cf 51 8e 7f 5e 29 67 3a cd bc 07 d6 bf 35 5e 11
Plain Text (64 bits)	01 23 45 67 89 ab cd ef
Cipher Text (64 bits)	8b 1d a5 f5 6a b3 d0 7c

TABLE II
Management of encryption sub-keys

B. Simulation

Before proceeding to the implementation on *FPGA*, we had to verify that our program was working correctly through *ISIM* simulation. The results of the simulations obtained are compared with the test reference data provided in [4], which are reported in the table II.

1) Simulation of the secret key management process: The secret key management program is based on the function FI (fig 3). It uses two S-Boxes S7 and S9. Once programmed in combinatorial logic, the results of the simulations of the two S-Boxes are compared to the two decimal tables reported in [4].

Simulation of the key management program makes it possible to both check the key management process itself and the correct programming of the FI function and the two S7 and S9 S-Boxes.

In the fig 9, the simulation results of the key management module are illustrated. For the same secret reference key K, provided in [4], we get the same sub-key K'.

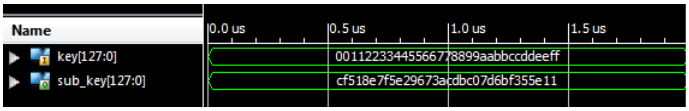


Fig. 9. Simulation result of the key management module under *ISIM*.

2) Simulation of the encryption procedure: Once the FI function program has been validated, we first programmed the FO function which is based on three functions FI and some logical operations (fig 6). Secondly, we programmed the function FL which is a series of simple logical operations. Thirdly, we have programmed the encryption sub-key management module.

Finally, and since all the components of MISTY1 have been programmed, we moved to programming the MISTY1 algorithm in encryption mode. Recall that the algorithmic structure of the program has been deduced from the fig 1.

Using the test reference data published in [4], we simulated the main program MISTY1 in encryption mode under $ISIM$. The simulation results are shown in Figure 10. Indeed, we introduced the plain text (*Plain-text*) and the secret key (*secrete-key*), given in the table II, to output the ciphertext (*cipher-text*) as a result.

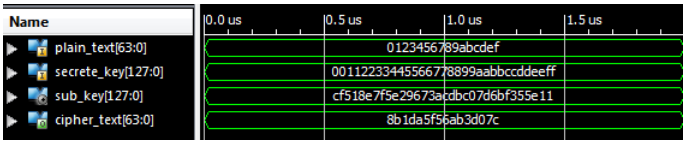


Fig. 10. Simulation results of the MISTY1 module in encryption mode.

3) Simulation of the decryption procedure: Once the algorithm MISTY1 is simulated in encryption mode, we switched to simulation of the algorithm in decryption mode. For this we made the following changes:

- Programming the function FL^{-1};
- Execute FL^{-1} function instead of FL function ;
- Reverse the order of sub-keys for decryption.

The program of the decryption is based on the flowchart shown in fig 2. The simulations resultsin decryption mode are presented in fig11. We can conclude that the original plaintext is recovered thanks to the introduction of the ciphertext at the input of the decryption block. we have been able to recover the original plaintext by introducing

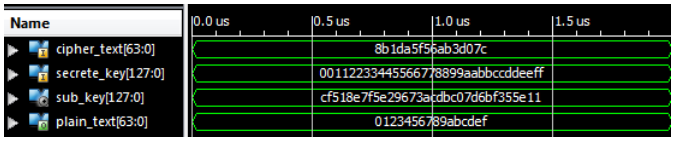


Fig. 11. Result of simulation of the MISTY1 module in decryption mode.

C. FPGA implementation and hardware verification

This section will cover the implementation of MISTY1 based on the development board ML507 which has the Xilinx Virtex 5 xc5vfx70t-1ff1136 FPGA chip.

1) The resource consumption: The resource consumption, after placement and routing of the algorithm give the results presented in table III.

Device Utilization Summary	
Selected device : *XC5vfx70t-1ff1136*	
Slice Logic Utilization	**Utilization**
Number of Slices Registers	01%
Number of Slices LUTs	15%
Number of fully used LUT-FF pairs	01%
Number of occupied slices	29%
Number of bonded IOBs	40%
Number of BUFG/BUFGCTRLs	01%
Maximum Frequency	20.934 MHz

TABLE III
RESOURCE CONSUMPTION OF THE MISTY1 PROGRAM ON FPGA XILINX VIRTEX 5 TYPE CIRCUIT.

Table III shows that the resources consumed by the studied algorithm are low compared to the resources available in the FPGA circuit, thanks to the simplicity of its architecture.

For a frequency of 20.934 MHz, a bit rate of 669.792 Mbps is obtained.

D. Implementation results

1) Encryption mode: After FPGA implementation, and using the $ChipscopePro$ tool, the results are given in fig 12. The data displayed on the visualization interface is identical to the reference data of the tests.

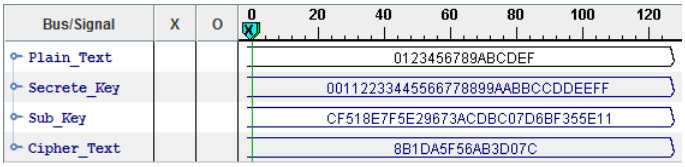


Fig. 12. Runtime results (under *ChipScope*) of MISTY1 in encryption mode.

2) Decryption mode: Once the execution of the hardware verification in encryption mode has been completed, we have implemented the decryption mode. Fig 13 shows the results of the implementation. We noticed that we were able to retrieve the plain text from the ciphertext text introduced as input to the decryption module.

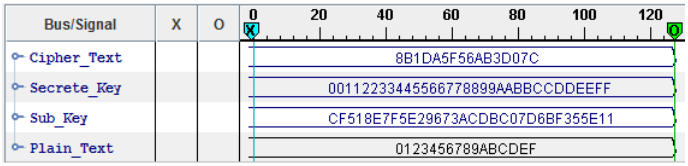


Fig. 13. Runtime results (under *ChipScope*) of MISTY1 in decryption mode.

IV. NIST STATISTICAL TEST RESULTS

To analyze and interpret the empirical results, we adopt the two approaches presented in [7]. The first approach is

the evaluation of the proportion of the sequences that have passed the various NIST tests. The second is to evaluate the distribution of P_value for each test, if one of these two approaches fails, the corresponding null hypothesis should not be rejected.

In the first approach, we calculate the proportion of the sequences that passed the test. For example, if there are 298 sequences that passed the test among the 300 sequences examined (m = 300) and the significance level $alpha = 0.01$, the proportion is equal to $p = \frac{298}{300} = 0.9933$. The confidence interval is determined by the following formula [7]:

$$p \pm 3\sqrt{(\frac{p \cdot \alpha}{m})} \quad with \quad p = 1 - \alpha \tag{42}$$

In our case the lower margin of the interval is equal to:

$$0.99 - 3\sqrt{(\frac{0.99 \cdot 0.01}{300})} = 0.972766 \tag{43}$$

The proportion should be above the lower margin set at 0.972766. So we can accept the null hypothesis, because 0.9933 is greater than 0.972766.

This approach can be illustrated by a graph representing the proportions of the sequences for each test. The sequences pass a test, if their proportion is above the lower margin represented in the graph 14.

The second approach is to examine the $P–values$ distribution of all sequences used for each test, to ensure consistency. It can be illustrated by a histogram, or an interval of 0 to 1 is subdivided into 10 subintervals. The $P–values$ are shared in the sub-ranges, for each sub-interval the frequency of $P–values$ is shown.

Uniformity can also be determined by applying the test χ^2 [7]. The distribution χ^2 is illustrated as follows:

$$\chi^2 = \sum_{i=1}^{10} \frac{(F_i - {}^{s}/_{10})^2}{{}^{s}/_{10}} \tag{44}$$

With F_i is the number of $P–values$ in the subinterval i, and s is the number of sequences used.

A. Generators studied

According to [8] [9], an implanted block cipher with a feedback of its output in its input can be considered as a random data generator. This why, we performed the NIST statistical tests on sequences generated from MISTY1.

B. First approach

The results of the NIST statistical tests obtained by the first approach, for the proposed generator , are presented in the table IV. The value presented in the table is the proportion of the sequences that pass each test successfully. As a reminder, this must be greater than 0.972766 to consider that the sequence satisfies the criteria of a random sequence.

The results obtained for the sequences generated by the algorithm tested by the first approach validate all 15 tests proposed by the NIST battery with proportions higher than 0.972766.

N°	designation of tests	Proportion
1	Frequency Test	0.9933
2	Block Frequency Test	0.9900
3	Cumulative Sums Test Up	0.9900
4	Cumulative Sums Test Up	0.9933
5	Runs Test	0.9867
6	Long Runs of Ones Test	1.0000
7	Rank Test	0.9900
8	Discrete Fourier Transform Test	0.9967
9	Non-overlapping Template Matching Test	0.9900
10	Overlapping Template Matching Test	0.9823
11	Maurer's "Universal Statistical" Test	0.9933
12	Approximate Entropy Test	0.9967
13	Random Excursions Test	1.0000
14	Random Excursions Variant Test	1.0000
15	Serial Test 1	0.9967
16	Serial Test 2	0.9800
17	Linear complexity Test	0.9823

TABLE IV
PROPORTION OF SEQUENCES THAT PASS EACH TEST SUCCESSFULLY

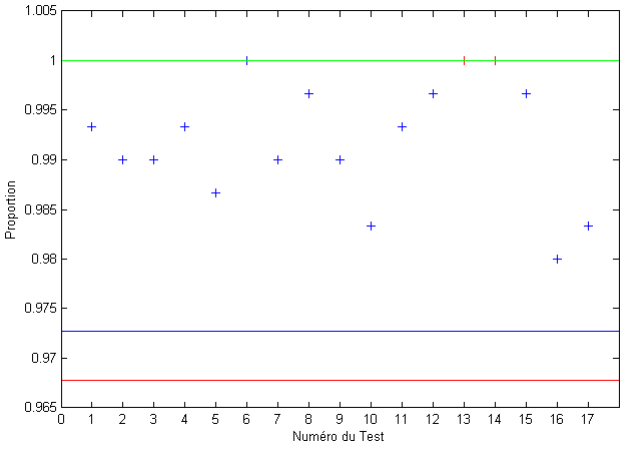


Fig. 14. Proportions of the sequences that pass each test successfully (MISTY1).

Fig 14 illustrates the proportion of sequences that pass each test with success for the binary sequences formed by the studied generator. We notice that the whole tests of NIST battery are upper at the lower margins for each generator.

C. Second approach

The NIST statistical tests results obtained by the second approach, for the generator studied, are given in table V. They show the values of the $P–values_T$. As a reminder, the $P–values_T$ allows us to examinate the distribution of the $P–values$ of each test, that must be greater than 10^{-4} to consider that the sequence satisfies the uniformity criteria.

The $P–values$ distribution of all tests is illustrated by histograms (fig 15). The histogram contains 10 sticks, each one has a width of 0.1 and a height defined by the number of occurrences of the $P–values$ in each interval, defined between

N°	Designation of tests	Total P-Value
1	Frequency Test	0.366918
2	Block Frequency Test	0.419021
3	Cumulative Sums Test Up	0.851383
4	Cumulative Sums Test Up	0.060239
5	Runs Test	0.209577
6	Long Runs of Ones Test	0.127148
7	Rank Test	0.055361
8	Discrete Fourier Transform Test	0.035174
9	Non-overlapping Template Matching Test	0.969347
10	Overlapping Template Matching Test	0.171867
11	Maurer's "Universal Statistical" Test	0.935716
12	Approximate Entropy Test	0.942865
13	Random Excursions Test	0.666014
14	Random Excursions Variant Test	0.839124
15	Serial Test 1	0.644060
16	Serial Test 2	0.540878
17	Linear complexity Test	0.129620

TABLE V
NIST STATISTICAL TEST RESULTS, PROPORTION OF SEQUENCES THAT PASS EACH TEST SUCCESSFULLY

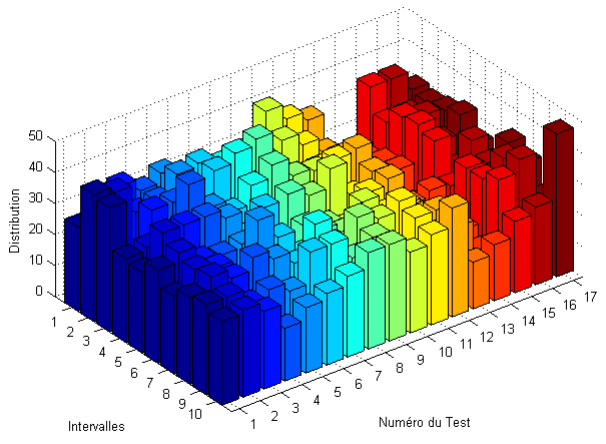


Fig. 15. $P–values$ distribution of MISTY1.

0 and 1 with a step of 0.1. The $P–values_T$ tells us about this uniformity (table V).

For our case, the uniformity of the $P–values_T$ is guaranteed since the number of occurrences in each ten intervals approaches the value "30", since the total of the sequences used for each test is equal to 300.

CONCLUSION

In this present paper, we presented the structure of the MISTY1 block cipher, and showing its components with a detailed description of the different functions used, either during the process of encryption-decryption or during the subkey management procedure.

We also presented the programming approach of the MISTY1 algorithm in VHDL language as well as a verification on the hardware by its implementation on FPGA board.

Firstly, we detailed the design approach of the program. Secondly, we coded the algorithm in VHDL language, we performed behavioral simulations under $ISIM$. The results were identical to the data test reference [4]. This results guaranteed that the code worked in both encryption and decryption mode. Thirdly, we moved to the experimental aspect, we implemented the algorithm on an FPGA board, and we were able to perform a hardware check using the built-in tool *Chipscope Pro*. we found that the bit rate is important and the resources consumed are low it offers slight avantages in terms of hardware cost. This makes it more suitable for hardware implementation. Finally, we evaluated the performances of the studied algorithm, in order to validate its security level.

The statistical analysis done by the NIST battery, for the binary sequences formed by the original MISTY1 algorithm keeps the same random character. Therefore, and relevant to our hypothesis, the results obtained for both approaches are consistent.

REFERENCES

[1] Kitsos, P., Galanis, M. D., Koufopavlou, O. (2004, May). High-speed hardware implementations of the KASUMI block cipher. In 2004 IEEE International Symposium on Circuits and Systems (IEEE Cat. No. 04CH37512) (Vol. 2, pp. II-549). IEEE.

[2] Imai, H., Yamagishi, A. (2011). CRYPTREC (Japanese Cryptographic Algorithm Evaluation Project). Encyclopedia of Cryptography and Security, 285-288.

[3] Preneel, B. (2011). NESSIE project. Encyclopedia of Cryptography and Security, 831-836.

[4] Matsui, Mitsuru. "New Block Encryption Algorithm MISTY." FSE (1997).

[5] Matsui, M. (2000). Supporting Document of MISTY1. version 1.1.

[6] Lai, X. Higher order derivatives and differential cryptanalysis. (p.227-233). Springer, Boston, MA.

[7] Bassham, L, E. Rukhin,A. L.Soto, J. Nechvatal, J. R... and Banks, D. L. (2010). Statistical test suite for random and pseudorandom number generators for cryptographic applications, NIST special publication.

[8] Schneier, B. Kelsey, J. Whiting, D. Hall, C. Ferguson, N. (1999) Performance comparison of the AES submissions.

[9] Hellekalek, P. Wegenkittl, S. (2003). Empirical evidence concerning AES. ACM Transactions on Modeling and Computer Simulation (TOMACS), 13(A), p322-333.

MINISTÈRE DE L'ENSEIGNEMENT
SUPÉRIEUR ET DE LA RECHERCHE SCIENTIFIQUE

UNIVERSITÉ DES SCIENCES ET DE LA TECHNOLOGIE D'ORAN - MOHAMED BOUDIAF

FACULTÉ DE GÉNIE ELECTRIQUE | DÉPARTEMENT D'ELECTRONIQUE
LABORATOIRE DE CODAGE ET DE LA SÉCURITÉ DE L'INFORMATION : LACOSI

18-19 JUIN 2019,
U.S.T.O-MB,
ORAN. ALGERIE

2'IWCA'19

Second International Workshop on Cryptography and its Applications

Deuxième International Workshop sur la Cryptographie et sur ses Applications

Organisée par l'USTO-MB

WWW.UNIV-USTO.DZ/2IWCA19/ IC2016CA@GMAIL.COM

00213 41627163 | 00213 664811717

SCAN ME

Second International Workshop on Cryptography and its Applications 2'IWCA'2019

جامعة العلوم والتكنولوجيا بوهران ــ محمد بوضياف

Université des Sciences et de la Technologie d'Oran Mohamed BOUDIAF
BP 1505 Oran El M'NAOUER.
www.univ-usto.dz