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

Second International WORKSHOP

International Workshop on Cryptography and its Applications

2'IWCA'19

on Cryptography and its Applications

Organisée par l'USTO-MB

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

ORAN. ALGERIE

PROCEEDING

DÉPARTEMENT D'ELECTRONIQUE, FACULTÉ DE GÉNIE ELECTRIQUE, U.S.T.O-M.B
BP 1505 EL M'NAOUER ORAN (31000) ALGÉRIE

CONTACT

Tél. & Fax : +213 41 62 71 63
Mobile : +213 664811717
E. mail: ic2016ca@gmail.com
Web site: https://www.univ-usto.dz/2IWCA19/

Our Sponsors & Supporters

Table of contents

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 Stockholom
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 Malaysian Journal of Applied Sciences (https://journal.unisza.edu.my/myjas/index.php/myjas) and International Journal of Information Security Science (http://ijiss.org/)

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.

Oral Session

Paper Number: 2'IWCA'19_ 02

Entitled: ***"Recognition of individuals from iris images using fusion methods and support vector Machine"***,

Authors: **Ghalem kamel Ghanem - Hendel Fatiha**

University of Sciences and Technology of Oran Mohamed Boudiaf, USTO-MB

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 Integro-differential operator. We conclude that Hough transform is performant than the Integro-differential 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

****

Paper Number: 2'IWCA'19_ 06

Entitled: ***"Efficient FPGA Implementation of Modular Multiplication and Exponentiation"***,

Authors: **M. Issad[1] – M. Anane[2] – B. Boudraa[3] – A. M. Bellemou[1] – N. Anane[1]**

[1]Centre de Développement des Technologies Avancées-CDTA
[2]Ecole Supérieure d'Informatique-ESI, Alger
[3]University of Houari Boumediene USTHB, Bab Ezzouar, Alger

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.

****

Paper Number: 2'IWCA'19_ 08

Entitled: ***"An Improved Encryption Approach Based on Multi-chaotic Maps Applied to Digital Image"***

Authors: **Lamiche Chaabane**

Mohamed Boudiaf University M'sila, Algeria

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.

****

Paper Number: 2'IWCA'19_ 09

Entitled: ***"*Secure Hybrid Crypto-system AES/RSA on FPGA for Data Communication"***

Authors: **M. Issad[1] – N. Anane[1]– A. M. Bellemou[1] – B. Boudraa[2]**

[1]Centre de Développement des Technologies Avancées-CDTA
[2]University of Houari Boumediene USTHB, Bab Ezzouar, Alger

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 that 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 a hybrid cryptography combining symmetric and asymmetric cryptographies. The security of server-client communications 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.

****

Paper Number: 2'IWCA'19_ 11

Entitled: ***"A New Approach to Verifying and Sharing a Secret QR Code using Elliptic Curves"***

Authors: **Hichem BOUCHAKOUR ERRAHMANI[1,2] - Hind IKNI[2]**

[1]Djillali Liabes University, Sidi Bel Abbes, Algeria
[2]Belhadj Bouchaib Center-University, Ain Temouchent, Algeria

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.

****

Paper Number: 2'IWCA'19_ 12

Entitled: ***"Security Enhancements of A5/1 Based Particle Swarm Optimization for Mobile Telecommunication Networks"***

Authors: **A. GHAZLI[1,2] – A. ALI-PACHA[2] – N. HADJ SAID[2] – B. Ghazli[1]**

[1]Tahri Mohamed University of Bechar, Algeria
[2]University f Sciences and Technology of Oran Mohamed Boudiaf, Algeria

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 and the random subgraph attack.

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 to 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

****

Paper Number: 2'IWCA'19_ 13

Entitled: ***"Nonstandard notes on the ratio of two expressions formed by the product and the sum of certain multiplicative arithmetic functions"***

Authors: **DJAMEL BELLAOUAR**

University of Guelma, Algeria

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.

****

Paper Number: 2'IWCA'19_ 14

Entitled: ***"A New Efficient Approach Based on Chaotic Map for Image Encryption"***

Authors: **Ali HADOUDA - Najia TRACHE - Mohamed Fayçal KHELFI**

University of Oran1 Ahmed Benbella, Algeria

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.

****

Paper Number: 2'IWCA'19_ 15

Entitled: ***"DNA Encryption Algorithm Based on Variable Coding Scheme"***,

Authors: **Mustapha MEFTAH - Adda ALI PACHA – Naima HADJ SAID**

University of Sciences and Technology of Oran – Mohamed Boudiaf- USTO-MB, Algeria

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.

****

Paper Number: 2'IWCA'19_ 17

Entitled: ***"Image encryption by AES algorithm based on chaos-Permutation"***,

Authors: **R. RIMANI[1,2] – N. HADJ SAID[2] – A. ALI PACHA[2] - J. A. López RAMOS[3]**

[1]University Mustapha Stambouli of MASCARA
[2]University of Sciences and Technology of Oran – Mohamed Boudiaf- USTO-MB, Algeria
[3]University of Almeria SPAIN

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.

****

Paper Number: 2'IWCA'19_ 19

Entitled: ***"Face Identification using Kinect Depth-Maps under One Sample per Person Scenario"***,

Authors: **Ahmed Yassine Boumedine –Samia Bentaieb – Abdelaziz Ouamri**

University of Sciences and Technology of Oran – Mohamed Boudiaf- USTO-MB, Algeria

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

****

Paper Number: 2'IWCA'19_ 20

Entitled: ***"A novel image encryption approach using polar decomposition and orthogonal matrices"***,

Authors: **Oussama Noui[1] – Amine Barkat[2] – Assia Beloucif[3] - Lemnaour Noui[3]**

[1]University of Batna1, Algeria, [2] Politecnico di Milano, Italy, [3]University of Batna2, Algeria

Abstract:

Information security is one of the important issues in the information age, image encryption algorithms have been increasingly studied to guarantee the secure image transmission over the inter-net 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 at-tacks (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

****

Paper Number: 2'IWCA'19_ 23

Entitled: ***"Privacy Analysis of a New Authentication Protocol for Internet of Things"***

Authors: **Noureddine Chikouche**

Mohamed Boudiaf University 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

****

Paper Number: 2'IWCA'19_ 25

Entitled: ***"A Clustering algorithm for distributing certificates in OLSR protocol"***,

Authors: **Mohammed Amine BOUDOUAIA[1,2] –Adda ALI PACHA[1] - Pascal LORENZ[2]**

[1]University of Sciences and Technology of Oran – Mohamed Boudiaf- USTO-MB, Algeria
[2]University of Haute Alsace, Colmar, France

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

****

Paper Number: 2'IWCA'19_ 27

Entitled: ***"Anonymous communication in IoT based on verifiable encryption"***,

Authors: **Khaled Hamouid**

University of Mostefa Ben Boulaid, Batna, Algeria

Abstract:

This paper proposes a pseudonym-based authentication scheme for Internet of Things (IoT). Based on the concept of verifiable encryption, this scheme is intended to protect privacy of users and support anonymous communications in IoT. This means that objects and users in the IoT may 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.

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.

Index Terms—IoT, verifiable encryption, authentication, anonymity, privacy

****

Paper Number: 2'IWCA'19_ 28

Entitled: ***"Chaotic Encryption for Fingerprint Images"***,

Authors: **Sabri Ahmed –Ouslim Mohamed**

University of Sciences and Technology of Oran – Mohamed Boudiaf- USTO-MB, Algeria

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 encryptions 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.

****

Paper Number: 2'IWCA'19_ 29

Entitled: ***"Efficient GeMSS Based Ring Signature Scheme"***,

Authors: **Murat Demircioglu[1] – Sedat Akleylek[2] - Murat Cenk[1]**

[1]Middle East Technical University Ankara, Turkey
[2]Ondokuz Mayis University Samsun, Turkey

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

****

Paper Number: 2'IWCA'19_ 33

Entitled: ***"Three-Weight Minimal Linear Codes and Their Applications"***,

Authors: **Sihem Mesnager[1] – Ahmet Sınak[2]- Oğuz Yayla[3]**

[1]University of Paris VIII, France
[2]Necmettin Erbakan University, Turkey
[3]Hacettepe UniversityAnkara, Turkey

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

****

Paper Number: 2'IWCA'19_ 34

Entitled: ***"New Signature Algorithm Based on Concatenated Rank Codes"***,

Authors: **Mahdjoubi Roumaissa[1] – Sedat Akleylek[2] - Guenda Kenza[1]**

[1]Univesity of Science and Technology Houari Boumediene, Algiers, Algeria

[2]Ondokuz Mayis University Samsun, Turkey

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. The robustness becomes from the hardness of the rank syndrome decoding (RSD) problem and the efficient decoding algorithm of their concatenation.

Index Terms—Rank metric, Signature algorithm, λ-Ganidulin code, LRPC codes.

****

Paper Number: 2'IWCA'19_ 40

Entitled: ***"Two new Quantum Attack Algorithms against NTRU pke # KA NTRU # & # PA NTRU #"***,

Authors: **EL Hassane LAAJI [1] - Abdelmalek AZIZI[1] – Siham AZZOUAK[2]**

[1]Mohamed First University, Oujda, Morocco
[2]Sidi Mahammed Ben Abdellah University, Fes, Morocco

Abstract:

The NTRU encrypt 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.

****

Paper Number: 2'IWCA'19_ 42

Entitled: ***"Efficient Hardware Implementation of Elliptic Curve Diffie-Hellman Key Exchange Protocol"***,

Authors: ***Mohamed SAOUDI**** – *Akram KERMICH - abdelfatah ZEBDA - Boufeldja ALLAILOU*

****Department of Electronics, ESACH/Algiers, Algeria***

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.

****

Paper Number: 2'IWCA'19_ 44

Entitled: ***"Hardware Acceleration of AES Cryptographic Algorithm for IPsec"***,

Authors: **/: *Omar Hocine BENHADDAD*** [*] **-** *Mohamed SAOUDI - Amine DROUICHE - Mohamed RABIAI - Boufeldja ALLAILOU*

[*]***Department of Electronics, ESACH/Algiers, Algeria***

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.

****

Paper Number: 2'IWCA'19_ 47

Entitled: ***"Implementation and statistical tests of a blockcipher algorithm MISTY1"***,

Authors: ***Sarah Moussaoui*** [*] **-** *Sabrina Zeghdoud - Boufeldja ALLAILOU*

[*]***Laboratoire Centrale de R&D, ECRMT/Algiers, Algeria***

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.

****

Poster Session

Paper Number: 2'IWCA'19_ 01

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

Authors: **Oualid Benamara**

USTHB, Institute of Mathematics, Algeiers

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.

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.

Index Terms—zero knowledge proofs, Reed Solomon codes

****

Paper Number: 2'IWCA'19_ 03

Entitled: ***"Modeling and non-linear dynamic analysis of the chaotic Colpitts oscillator up to 1 GHz"***,

Authors: **Chahira Rouifed[1] - Achour Ouslimani[2] - Mourad Laghrouche[1]**

[1] University of Mouloud Mammeri - 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

****

Paper Number: 2'IWCA'19_ 05

Entitled: ***"Proposition of a New Vernam Chaotic Cipher"***,

Authors: **Hana ALI PACHA – Naima HADJ SAID – Adda ALI PACHA**

University of Sciences and Technology of Oran – Mohamed Boudiaf- USTO-MB, Algeria

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

****

Paper Number: 2'IWCA'19_ 07

Entitled: ***"A Presentation of a Linear Code over:*** $\mathcal{A}_{q,3} = \mathbb{Z}_q[u_1, u_2, u_3] / \langle u_i^2 = 1, u_i u_j = u_j u_i \rangle$ **„**

Authors: **Karima. Chatouh**

Mostefa Ben Boulaid University, Batna 2, Algeria

Abstract:

In this work, we introduce some explicit construction of codes over $\mathcal{A}_{q,3} = \mathbb{Z}_q[u_1, u_2, u_3] / \langle u_i^2 = 1, u_i u_j = u_j u_i \rangle$ 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.

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.

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

****

Paper Number: 2'IWCA'19_ 10

Entitled: ***"On public key cryptosystem based on the word problem in a group"***

Authors: **Nacer Ghadbane**

Mohamed Boudiaf University M'sila, Algeria

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 $s_{i_1}^{k_1} s_{i_2}^{k_2} ... s_{i_n}^{k_n}$ in 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.

****

Paper Number: 2'IWCA'19_ 18

Entitled: ***"New Technique of styganography based on the Theory of Chaos : Survey"***,

Authors: **Abdelkader Bouguessa – Naima HADJ SAID – Adda ALI PACHA**

University of Sciences and Technology of Oran – Mohamed Boudiaf- USTO-MB, Algeria

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.

****

Paper Number: 2'IWCA'19_ 21

Entitled: ***"Community structure in complex networks based on Tabu Search"***,

Authors: **Bilal SAOUD**

University of Bouira, Algeria

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

****

Paper Number: 2'IWCA'19_ 22

Entitled: ***"SIMULATION OF ATTACKS ON AUTHENTICATION PROTOCOLS FOR NEAR FIELD COMMUNICATIONS"***

Authors: **Noureddine Chikouche**

Mohamed Boudiaf University 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

****

Paper Number: 2'IWCA'19_ 24

Entitled: ***"Approach Management Application in Cloud Computing: Runtime vs Docker"***

Authors: **Asmaa Aouat - El Abbassia Deba - Abou El Hassan Benyamina**

University of Oran1 Ahmed Benbella, Algeria

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.

****

Paper Number: 2'IWCA'19_ 26

Entitled: ***" Double Skew (1+u) – Constacyclic codes over***  ***"***,

Authors: **Ahlem Melakhessou[1] – Kenza Guenda[2]**

[1]*University of Mostefa Ben Boulaid, Batna, Algeria*
[2]*University of Houari Boumediene USTHB, Alger, Algeria*

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.

****

Paper Number: 2'IWCA'19_ 30

Entitled: ***"A Different Encryption System Based on the Integer Factorization Problem"***,

Authors: **Karima Djebaili[1] – Lamine Melkemi[2]**

[1]University of Ouragla, Algeria
[2]Mostafa Ben Boulaid, Batna, Algeria

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.

****

Paper Number: 2'IWCA'19_ 31

Entitled: ***"Lifted Codes over Finite Chain Rings"***,

Authors: **Reguia Lamia Bouzara[1] – Edgar Martinez-Moro[2]- Kenza Guenda[1]**

[1]University of Houari Boumediene USTHB, Alger, Algeria
[2]University of Valladolid, Spain

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.

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.

Index Terms—valuation rings, finite chain rings, lifted codes.

****

Paper Number: 2'IWCA'19_ 35

Entitled: ***"Encrypting the TCM Encoder with Locally Rotated Constellations in Rayleigh Fading Channel"***,

Authors: **Rekkal kahina[1] – Rekkal Sarah[2]- Abdesselam Bassou[1]**

[1]Tahri Mohamed University, Bechar, Algeria
[2]Ahmed Benbella University 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.

****

Paper Number: 2'IWCA'19_ 36

Entitled: ***"Secure MD4 Hash Function Using Henon Map"***,

Authors: **Amine Zellagui – Naima HADJ SAID – Adda ALI PACHA**

University of Sciences and Technology of Oran – Mohamed Boudiaf- USTO-MB, Algeria

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.

****

Paper Number: 2'IWCA'19_ 37

Entitled: ***"Using of Multi Chaotic System for Implementing a Good Cryptosystem"***,

Authors: **Khalfallah ALI CHERIF – Naima HADJ SAID – Adda ALI PACHA**

University of Sciences and Technology of Oran – Mohamed Boudiaf- USTO-MB, Algeria

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

****

Paper Number: 2'IWCA'19_ 38

Entitled: ***"Detection and Prevention of Suicidal Self-harm Behavior in Twitter"***,

Authors: **Hadj Ahmed BOUARARA**

Moulay Tahar University , 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.

****

Paper Number: 2'IWCA'19_ 39

Entitled: ***"PSO Variants for Localization Challenge in Wireless Sensor Network and Internet Of Thing"***,

Authors: **L. BAIDAR[1] – A. RAHMOUN[1] – P. LORENZ[2] – M. MIHOUBI[3]**

[1]Ecole Supérieure en Informatique ; Sidi Bel Abbes, Algeria
[2]University of Haute Alsace, Mulhouse, France
[3]Djillali Liabes University, Sidi Bel Abbes , Algeria

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.

****

Paper Number: 2'IWCA'19_ 41

Entitled: ***"Study On Skew Codes over The ring Zq + uZq"***,

Authors: **Hebbache Zineb[1] –Kenza Guenda[1,2]**

[1]University of Houari Boumediene USTHB, Alger, Algeria
[2]University of Victoria, Canada

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 *Zq* 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.

****

Paper Number: 2'IWCA'19_ 43

Entitled: ***"Authentication, Cyphering & Security in Modern Mobile Network"***,

Authors: **Salah Salim Belaifa**

Technology/ T.NOC.Transmission, Djezzy Telecom Algeria

Abstract:

In This paper we present the notion of authentication, Cyphering 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.

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

Keywords — Signaling, Authentication, Cyphering & IT.Security.

****

Paper Number: 2'IWCA'19_ 45

Entitled: ***"Hand Biometry: A Review"***,

Authors: **Farah Bahmed[1,2] –Madani Ould Mammar[2,3]**

[1]Ahmed Zabana University Centre, Relizane,, Algeria
[2]University of Sciences and Technology of Oran, Mohamed Boudiaf, Algeria
[3]University Abdelhamid Ibn Badis, Mostaganem, Algeria

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.

Multi-biometric 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.

****