SOUS LE HAUT PATRONAGE DE MONSIEUR LE MINISTRE DE L'ENSEIGNEMENT SUPÉRIEUR ET DE LA RECHERCHE SCIENTIFIQUE

UNIVERSITÉ DES SCIENCES ET DE LA TECHNOLOGIE D'ORAN - MOHAMED BOUDIAF

International

Workshop

sur la Cryptographie et sur ses Applications

Organisée par l'USTO-MB

26-27 AVRIL 2016,

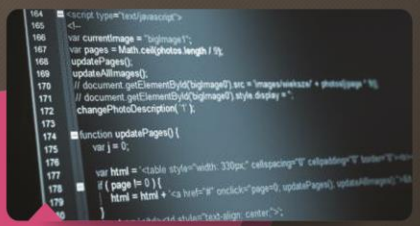
U.S.T.O-MB, ORAN. ALGERIE

International Workshop on Cryptography and its Applications

IWCA '16

Proceeding

Cryptographie



Contacts: : 00 213 41560329

00 213 664811717

http://www.univ-usto.dz/ICCA1/

Département d'Electronique, Faculté de Génie Electrique, U.S.T.O-M.B

BP 1505 EL M'Naouer Oran (31000) Algérie

University of Sciences and Technology of Oran - Mohamed Boudiaf -

Electrical and Electronics Engineering Faculty

Electronics Department

The 5th International Workshop on Cryptography and its Applications - IWCA' 2016

April 26 – 27, 2016 – Oran, Algeria

Table of contents

WELCOME MESSAGE FROM THE CONFERENCE CHAIR

It's a great pleasure and honor for me to welcome you all to IWCA'2016, International Workshop on Cryptography and its Applications, being held here at Algerian University of Sciences and Technology of Oran-MB, Electrical Engineering Faculty, Electronics Department.

The main objective of this workshop is to provide an update on the latest advances in cryptography and computer security: methods, technologies and applications. This workshop is for the national university research community, first and participating in industrial developments in data security and their implementation on the constraints and design methods related to this activity.

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

Algerian Democratic and Popular Republic

Ministry of Higher Education and Scientific Research

University of Sciences and Technology of Oran - Mohamed Boudiaf-

Electrical and Electronics Engineering Faculty

Electronics Department

International Workshop on Cryptography and its Applications - IWCA' 2016

Oran, 26 & 27 April 2016

Call for Papers

Dear colleagues,

This international workshop will take place between 26 and 27 April 2016 at the University of Sciences and Technology of Oran Mohamed Boudiaf, Algeria. Oran.
The aim of this conference is to provide an update on the latest advances in cryptography and computer security: methods, technologies and applications.
This conference is for the national university research community, first and participating in industrial developments in data security and their implementation on the constraints and design methods related to this activity.
This conference aims to establish contacts between university researchers and entrepreneurs in such a way to launch effective cooperation between the two parties in the interest of the development of local and national industry.

Major objectives

A. Promoting knowledge exchange and experiences among national and international researchers;
B. Reflection in the creation of an Algerian Association for Cryptography;
C. The initiation of national and international cooperation between universities and industry in the field of security in telecommunications.
D. Companies working in the field of electronic engineering (smart card and RFID), are invited to exhibit their products and services at this conference.

Honorary President of the conference: The Rector of the USTO-MB, Prof. Benharrats Nacéra
Honorary Chairman: Prof. Brahim Abelhalim Taib. Dean of the Faculty of Electrical Engineering
Conference Chair: Prof. Adda Ali Pacha

Conference topics

- Cryptographics standards and applications
- Cryptanalysis
- Cryptographic algorithms, their design and implementation FPGA
- Cryptography and legislation
- Quantum and Post Quantum cryptography
- Privacy enhancing technologies
- Provable security
- RFID - security and cryptography aspects, etc.
- 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
- Watermarking
- Malware and Viruses,
- Wireless Network Security (Internet, WSNs, UMTS, WiFi, WiMAX, WiMedia and others)

Steering Committee

1. Ait Derna Abdelwahab
2. Alshaqaqi Blal
3. Bettahar Salim
4. Daoud Amine
5. Djelloul Mazouz Lakhdar

Scientific Committee

1. Abdelmalek Amine, Univ. Saida, Algeria
2. Ait Saadi Karima, CDTA, Algeria
3. Amroune Abdelaziz, Univ. Msila, Algeria
4. Arnault Francois, univ. Limoges, France
5. Azhari Abdelhak (E N S, Casablanca), Morocco
6. Barbot Jean Pierre Univ-Cergy Pointoise, France
7. Bayram Mustafa, Yildiz Technical Univ. Turkey
8. Belbachir Med Faouzi USTO- Oran, Algeria
9. Benmohamed Mohamed, Univ. Const. Algeria
10. Benslama Malek, Univ. Constantine, Algeria
11. Betina Kamel, USTHB, Algeria
12. Berrached NasrEddine USTO- Oran, Algeria
13. Boughaba Soraya, Univ. Constantine, Algeria
14. Bouhlel Med Salim, univ. Sfax, Tunisia
15. Bouridane Ahmed, Queen's University Belfast, UK
16. Carlet Claude, Univ. Paris 8, France
17. Derbal Ali, ENS Kouba , Algeria
18. Di Gennaro Stefano, Univ. Aquila, Italia
19. EL HAJJI Said, Univ. Med. V, Rabat, Morocco
20. Feham Mohamed, Univ. Tlemcen, Algeria
21. Feraoun Kamel Univ. Sidi Belabes, Algeria
22. Fouquet Mireille, Univ. Paris 7, France
23. Fournier-Prunaret Danièle, Univ.Toulouse, France
24. Gaborit Phillipe, Univ. Limoges, France
25. Ghanes Malek, Univ-Cergy Pointoise, France
26. Ghoualmi-Zine Nacira, Univ. Annaba, Algeria
27. Guenda Kenza, USTHB, Algeria
28. Guillot Philippe, Univ. Paris 8, France
29. Hadj Said Naima, USTO Oran
30. Hamri Nasreddine, Univ. Mila, Algeria
31. Hendel Fatiha USTO- Oran, Algeria
32. Larger Laurent, Univ-fcomte, France
33. Loukil Abdelhamid, USTO-Oran, Algeria
34. Lozi René Univ-Nice, France
35. Merazka Fatiha, USTHB, Algeria
36. Mesnager Sihem, Univ. Paris 8, France
37. Meziane Abdelkrim CERIST Alger, Algeria
38. M'hamed Abdallah Télécom SudParis France
39. Mokrane Abdellah, Univ. Paris 8, France
40. Nait Abdeslam Farid Univ-Paris 5, France
41. Nitaj Abdelrahman, Univ. Caen, France
42. Nouali Omar,CERIST Alger, Algeria
43. Noui Lemnaouar Univ. Batna, Algeria
44. Ould Mammar Madani, Univ. Mosta. Algeria
45. Ouamri Abdelaziz, USTO- Oran, Algeria
46. Ouslim Mohamed, USTO- Oran, Algeria
47. Puech William, Univ. Montpellier, France
48. Rahmoun Abdelatif, ESI. SBA, Algeria
49. Safwan El Assad, Univ-Nantes, France
50. Sedat Akleylek, Ondokuz Mayıs University, Samsun, turkey
51. Serres Jacques, Ecole Centrale de Lille, France
52. Talhi Chamseddine, Ecole de Technologie Supérieur, Québec, Canada
53. Tbahriti Salah-Eddine, CTS Oran, Algeria
54. Zedam Lemnaouar Univ. MSila, Algeria
55. Zeraoulia Elhadj, Univ. Tébessa, Algeria
56. Zribi Amin, ISET'COM, Tunisia

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.
Authors interested in this conference are invited to submit their proposals to full articles in PDF or Word format in one of two languages, English or French/Arabic (the summary must be in both languages), mentioning it electronically title of the paper, affiliations and email address. Articles should not exceed 08 A4 pages, single-spaced, in Times New Roman (TNR) 10.

A special issue of the journal RIST, published by CERIST, will be devoted to this event.

The submission site is open at: https://easychair.org/conferences/?conf=icca16

Important deadlines

31/01/2016: Submission of the complete article
02/18/2016: Notification of acceptance of the article
03/27/2016: Camera ready, final version of the article

Registration fees

Author participant: 2000 DA
Student: 1000 DA
Foreigners: 100 Euros
Other: 8000 DA

Participation fee covers accommodation, catering, breaks Cafes and acts of the conference.

Contacts

For further information contact:

Secretariat of the Conference IWCA'16
Department of Electronics, Faculty of Electrical Engineering, USTO-MB
BP 1505 EL M'Naouer Oran (31000) Algeria
Tel. & Fax: 00 213 41 560329 Mob. : 00 (213) 664811717
00 213 41 560301

E. mail: icca2016@univ-usto.dz et/or ic2016ca@gmail.com
Web site: http://www.univ-usto.dz/ICCA1/

University of Sciences and Technology of Oran - Mohamed Boudiaf

Electrical and Electronics Engineering Faculty

Electronics Department

International Workshop on Cryptography and its Applications

- IWCA' 2016-

Oran- 26 & 27 April 2016

PROGRAMME

Monday, April 25th

Special session for Master CSD Students

A. Ali-Pacha / W. Ait-Derna

90:00-12:00	Guillot Philippe, (**Univ. Paris 8**)	Cartes à puces

12:00-14:30	**Lunch**

14:30-17:30	Guillot Philippe, (**Univ. Paris 8**)	Cartes à puces

---

Tuesday, April 26th

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

Plenary Session 1

Co-Chairs: L. Noui / N. Berrached

10:00-10:50	René Lozi, (**Univ. Nice Sophia Antipolis, Fr.**)	Le futur prometteur de la théorie du chaos pour la Sécurité Cryptographique Personnelle

11:00-11:30	**Coffee Break**

Plenary Session 2

Co-Chairs: F. Belbachir / A. Ouamri

11:30-12:15	Safwan El Assad, (**Polytech Nantes, Fr.**)	Chaos-based- Information Hiding and Security: an emergent technology

Poster Session 1

Co-Chairs: M.Keche/ M. OuldMammar

12:15-12:45	**Poster Session 1**

12:45-14:00	**Lunch**

Oral Session 1

Co-Chairs: A. Kaddour / Z. Derouiche

14:00-14:20	OuerdiaMegherbi, Sarah Kassim, Hamid Hamiche, SaïdDjennoune (**Univ. Tizi-ouzou**)	A New Robust Hybrid Transmission Scheme based on the Synchronization of Discrete-Time Chaotic Systems
14:20-14:40	Karima Djebaili, Lamine Melkem,(**Univ. Batna**)	A NovelAlgorithm for Image EncryptionBased on Matrix Transformation
14:40-15:00	Sarah Kassim, Hamid Hamiche, SaıdDjennoune, OuerdiaMegherbi, (**Univ. Tizi-ouzou**)	A novel robust image transmission scheme based on fractional-order discrete chaotic systems
15:00-15:20	S. Benzegane, S. Sadoudi and M. Djeddou, (**EMP-Alger**)	Hyperchaos-Based Multimedia Encryption for Device-to-Device Communications
15:20-15:40	**1)** Slimani Dalila, Merazka Fatiha, (USTHB-Alger)	Cryptage Chaotique du Signal Parole

15:40-16:00	**Coffee Break**

Oral Session 2

Co-Chairs: Co-Chairs:N. Boughanmi/ M. Ouslim

16:00-16:20	Amine Rahmani, A. Amine, R. M.Hamou, M.ElhadiRahmani, M.A.Boudia, (**Univ. Saida**)	Genetic Algorithms Based model for Amelioration of TSZ Cryptosystem
16:20-16:40	AzzouziOussama, Anane Mohamed and Issad Mohamed, (**CDTA- Alger**)	Flexible Hardware/Software implementation of AES on FPGA
16:40-17:00	BOUCHERK Kahina, AMEUR Zohra, (**Univ. Tizi-Ouzou**)	Biometry based on retinal analysis
17:00-17:20	Nour El Houda A. MERABET, Redha BENZID, (**Univ. Batna**)	A Fragile watermark based on shortened BCH (16,11) for n out of n secret sharing scheme
17:20-17:40	**2)** CHERIF Amina, Damien Sauveron,(Univ. Tizi-ouzou)	Overview on Formal Verification Methods for RFID Protocols
17:40-18:00	R. DJELLAB,M. Benmohamed(**Univ. Batna**)	Verification of A Group Key Distribution Protocol based on QKD

Wednesday, April 27th

Plenary Session 3

Co-Chairs: M. Feham/ K.M.Ferouan

8:30-9:15	J.P. Barbot, (**ENSEA. Cergy-Pointoise, Fr.**)	Quelques éléments de la théorie du contrôle utiles pour la récupération et la transmission de l'information

Plenary Session 4

Co-Chairs: M. Benmohamed/ Abdelmelek Amine

9:15-10:00	SedatAkleylek, (**Univ. OndokuzMayis, Samsun, Turkey**)	Efficient Methods for Lattice-based Cryptography
10:00-10:20	**Coffee Break**	

Poster Session 2

Co-Chairs: H.Loukil/ F. Hendel

10:20-10:50	Poster Session 2

Oral Session 3

Co-Chairs: M.Bouzit / S. Soudani

10:30-10:50	A. Souyah, K.M. Faraoun, (**Univ. Sidi-Belabes**)	Symmetric ciphers for digital images: An Experimental Comparison Study
10:50-11:15	SamiaBentaieb and AbdelazizOuamri,**(USTO**)	3D Partial Face Recognition using Local Descriptors
11:15-11:35	GhazliAbdelkader, N. Hadj-Said, A. Ali-Pacha, (**USTO**)	Strong Genetic Stream Cipher Design to Secure Mobile Phone Telepony
11:35-11:55	AssiaBeloucif, LemnouarNoui, (**Univ. Batna**)	Une nouvelle stratégie de chiffrement d'images
12:00-12:50	**3)** Oussama Noui and LemnouarNoui, (Univ. Batna)	Sharing secret based on MDS codes for image encryption

Cloture Session

Co-Chairs: A. Ali-Pacha / N. Berrached

13:00-13:30	**Cloture and recommendation**

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

POSTER SESSION 1

Tuesday, April 26th

12:15-12:45	HentabliWahiba, Merazka Fatiha, (**USTHB-Alger**)	Software Implementation of an extended RSA Cryptosystem based on binary exponentiation
	Ouassila HOCEINI, (**Univ. Tizi-ouzou**)	A new Trust framework for Wireless sensor networks based Internet of things (TWI)
	NouaraMokhtari, (**Univ. Boumerdes**)	Negacyclic Codes Over Z4 + uZ4 + u^2Z4
	Aicha Batoul, Kenza Guenda, (**USTHB-Alger**)	Repeated-Root Constacyclic Codes over Finite Fields.
	Ines Khacheba, Mohamed BachirYagoubi,(**Univ. Laghouat**)	Conditional Privacy Preservation for VANET Safety Applications
	Nacer GHADBANE, Douadi MIHOUBI, (**Univ. M'Sila**)	Etude d'un système de cryptage basé sur le problème du mot dans un monoïde libre
	razika SOUADEK, N. Boukezzoula (**Univ. Setif**)	A robust watermarking scheme using a SVD technique and Differential Evolution in the algorithm of compression JPEG 2000
	4) K. Ait Saadi, B.Yahya-Zoubir, (CDTA-Alger)	Motion detection based motion saliency detection
	5) S. Selmane, A. ZIDANI, (Univ. Batna)	Situated Work Analysis of Attribute-Based Encryption (ABE): Case of Healthcare
	6) M. KHITAS, L.ZIET,F.RADJAH, (Univ. Setif)	FPGA design and Implementation of Histogram Algorithm for image processing
	Y. Zarouk, S.Souici, H.Seridi,(**Univ. Guelma**)	Algorithme de Cryptage Symétrie pour Les Données Multimédias Utilisant OEP
	I.Talbi,S. Boughaba,(**Univ. Constantine)**	Le chiffrement par blocs à base du chaos: un aperçu
	W.Issaadi, (**Univ.Bejaïa**)	CryptoPage: vers la fin du piratage informatique?
	NouaraZoubir and Kenza Guenda, (**USTHB-Alger**)	Some Results on Permutation Polynomials over Finite Fields
	R. Hamza, F. TITOUNA, (**Univ. Batna**)	A new pseudo random sequence generator based on the chaotic system chen
	A.Toumi, R. Adjoudj,(**Univ. Sidi-Belabes**)	AUTHENTIFICATION BIOMETRIQUE
	A.Merzoug, A. Ali-Pacha, N.Hadj-Said, (**Univ. Batna**)	Construction d'une Suite aléatoire par le biais de la Carte PWLCM : Application au chiffrement RC4

POSTER SESSION 2

Wednesday, April 27th

10:20-10:50	Ghalemkamelghanem&Hendelfatiha, (**USTO**)	Segmentation Techniques for Iris Recognition System
	Islem Ghaffor,**(USTO**)	The relation between counting primes and twin primes
	R. RIMANI, N.Hadj-Said, A. Ali-Pacha, (**USTO**)	Sécurisation des images par une combinaison de technique de chiffrement AES et de recalage d'image
	M. A.Boudia, R. M.Hamou, A. C.Lokbani, A. Amine, A.Rahmani, (**Univ. Saida**)	A new meta-heuristics for Intrusion Detection System by scenario inspired from the protection system of social bees
	H. A.Bouarara, M. R. HAMOU, A. Amine, (**Univ. Saida**)	New Private Information Retrieval using combination of filters based social workers bees' algorithm
	H.Bendouma, A. Ali-Pacha, N.Hadj-Said, (**USTO**)	Implémentation sur un circuit FPGA du Générateur Blum-Blum-Shub en vue de son application à la Cryptographie
	M. A .Filali, (**USTO**)	Etude et Implémentation Pipeline Sur FPGA de L'algorithme De Chiffrement AES
	7) A. Belaidi, M.A. Abderrahim, (Univ. Tlemcen)	Vers l'implémentation d'un modèle de contrôle d'accès pour les systèmes d'informations en santé
	Benmessaoud Nabila, A. Ali Pacha, N. Hadj Said, (**USTO**)	Application de la Transformée de Fourier pour la sécurité des images
	M. M. MIROUD, K. BELKADI, (**USTO-MB**)	Schéma de contrôle d'accès aux données médicales dans les systèmes e-santé basé sur le TOTP

Overview on Formal Verification Methods for RFID Protocols

Amina Cherif [1], Damien Sauverony [2] and Malika Belkadiz [1]
[1]Université de Tizi Ouzou, Laboratoire LARI, Computer Science Department, Algeria
[2]Université de Limoges, XLIM UMR CNRS 7252 – Mathematics and Computer Science Department, Limoges, France

Abstract
Cryptography plays an important role to ensure security and privacy protection in RFID systems. However, due to economical reasons for market penetration of RFID technologies, tags resources (i.e. computational and memory capabilities) are highly constrained. In this context, cryptographic protocols must rely on lightweight primitives. Since lot of proposed protocols are error-prone, in this paper, we focus on formal verification methods and study their use to detect flaws and/or verify the correctness of these RFID protocols.

Keywords: RFID, lightweight cryptographic protocols, threats, attacks, formal verification. Réf :01_31

Segmentation Techniques for Iris Recognition System

Ghalem kamel ghanem
Université des Sciences et de la Technologie d'Oran.
Mohamed Boudiaf-BP. 1505 EL M'Naouer 31000 Oran- Oran, Algérie.
Hendel fatiha
Université des Sciences et de la Technologie d'Oran.
Mohamed Boudiaf-BP. 1505 EL M'Naouer 31000 Oran- Oran, Algérie.

Abstract
Iris segmentation is foremost part of iris recognition system. There are four steps in iris recognition: segmentation, normalization, encoding and matching. This paper analyze the performance of Daugman Integrodifferential Operator as the most reliable segmentation technique compared to Hough Transform designed by Libor Masek in terms of accuracy and time complexity. Indeed, the obtained result shown that Integro-Differential Operator is more accurate than Hough Transform method with rate of 91.86% against 72.28% and also more faster with time of 12.49 minutes against 15.09 minutes testing on entire challenging UBIRIS v1 database (1205 iris images).

Keywords: segmentation; recognition; Daugman Integrodifferential Operator ; Hough Transform.
Réf :02_01

Symmetric ciphers for digital images: An Experimental Comparison Study

Souyah Amina, Faraoun Kamel Mohamed
Computer Science Department
Djilalli Liabes University
Sidi Bel Abbès, Algeria

Abstract
Due to the ever-increasing demand of secure schemes that are suitable in use for real-time Internet image encryption and transmission applications, different strategies are investigated in the literature among which: chaos theory and cellular automata. These mathematical models are used as bases to respond to the challenging issue of designing image encryption schemes that make a good compromise between speed and satisfactory level of security. The intend of this paper is to give an experimental comparison study between some of recent and prevalent existing schemes in the literature and our already proposed one. This study puts a focus on analyzing the performance of each scheme in terms of security level and speed.

Keywords: Cryptography, image encryption, chaotic systems, randomized encryption, diffusion. Réf :03_03

Sécurisation des images par une combinaison de technique de chiffrement AES et de recalage d'image

Rachid RIMANI, Naima HADJ SAID et Adda ALI-PACHA
Université des Sciences et de la Technologie d'Oran Mohamed Boudiaf USTOMB
BP 1505 El M'Naouer Oran 31036, ALGERIE

Abstract
Le chiffrement d'information a été utilisé comme instrument de sécurisation pour des stratégies militaires et des échanges de données secrètes. Aujourd'hui, les réseaux numériques ont fortement évolué ces dernières années et sont devenus inévitables pour la communication moderne. En fait, l'utilisation d'un réseau de communication expose les échanges à certains risques, qui nécessitent l'existence de mesures de sécurité adéquates. Par exemple, les images à transmettre peuvent être enregistrées et copiées durant leur parcours sans pertes de qualité. Les images piratées peuvent être par la suite le sujet d'un échange de données et de stockage numérique illégal. Il est donc nécessaire de développer un outil de protection efficace des données transférées contre les intrusions arbitraires. Le cryptage des données est très souvent le seul moyen efficace pour répondre à ces exigences.
Dans cet article, nous proposons un système symétrique de cryptage permettant de transférer des images de manière sécurisée on utilisant l'algorithme de chiffrement AES (Advanced Encryption Standard) en mode CBC (Cipher Block Chaining) combiné avec un système de recalage d'image afin d'améliorer le niveau de sécurité.

Keywords : cryptographie ; clé ; système symétrique ; chiffrement AES ; mode CBC, recalage d'image.
Réf :04_04

Flexible Hardware/Software implementation of AES on FPGA

Azzouzi Oussama [1], Anane Mohamed [2] and Issad Mohamed [1]
[1] Centre de Développement des Technologies Avancées CDTA Baba Hassen, Alger, Algérie
[2] Ecole nationale Supérieur d'Informatique ESI Oued Smar Alger, Algérie

Abstract
This paper presents the implementation on a high performance PSoC (Programmable System on Chip) for the AES (Advanced Encryption Standard). The sub keys generation (*Key Expansion*) is made by software and performed on the MicroBlaze processor. The encryption/decryption operations are made by a dedicated hardware IP (Intellectual Property) cores. This last is optimized at the low level LUT (Look up table) to accomplish the AES rounds with high throughput rate. This makes our system suitable to encrypt/decrypt large data. The system is implemented on Virtex 5 FPGA board and monitored by a Java software application which allows the connection and the communication with the PC. The proposed design operates at 100 MHz with 1023 slices as occupied area on the FPGA.

Keywords: AES, FPGA, Codesign, Key Expansion, MicroBlaze. Réf :05_07

Verification of A Group Key Distribution Protocol based on QKD

Rima DJELLAB, LAMIE lab, Mathematics and Computer Sciences Faculty, Computer Sciences department, University of Batna, Batna2.
Mohammed BENMOHAMMED, LIRE lab, NTIC Faculty, Software Technologies of Information and Communication Department, University of Constantine2.

Abstract
Key distribution is a core building block for secure communication. In group communication, key distribution is not a simple extension of two-party communication. Many approaches were proposed in the classical field, but those proposals are still based on the assumption that some computational problems are hard. Based on quantum mechanics lows, new field emerges allowing to generate and share a secret and secure key between two, or more, participants. In this paper, we propose new multiparty key distribution protocol in group communication based on the well-known quantum key distribution protocol BB84. The security of the proposed solution is based on the unconditional security of the BB84 allowed by the mechanics lows and the mathematical proved secure operation, XOR. In proposed solution each participant collaborates with a partial key in order to obtain at the end of the protocol the same group key that can be used for encryption aims. We also analyze and verify some security properties of the proposed protocol. This is done using a probabilistic symbolic model-checker, the PRISM tool.

Keywords: BB84; key management; PRISM model-checker; quantum key distribution; QKD in group; security; verification. Réf :06_08

Genetic Algorithms Based model for Amelioration of TSZ Cryptosystem

Amine Rahmani, Abdelmalek Amine, Reda Mohamed Hamou,
Mohamed Elhadi Rahmani, Mohamed Amine Boudia
GeCode Laboratory, Department of Computer Science
Tahar Moulay University of Saida Algeria

Abstract
The development of new technologies had led to the appearance of small and powerful computing devices (smart phones and internet of things). In the other side, the coming of big data and cloud computing had opened a new area of sharing and managing data from distance. This developments had given the birth of new challenges in term of information security and privacy of users. Many solutions have been proposed at this stage. One of the solutions was a specific crypto-graphic systems known as homomorphic encryptions. These last allow the treatment of encrypted data with-out need to decrypt it which conserve a high level of security. In the other hand, the domain of metaheuristics and bio-inspired had appeared with new algorithms that had proved a high efficiency in solving several problems of information technology including cryptography. Among the different techniques of data mining, there was the evolutionary computations inspired from the principles of biological evolution. This paper covers the problem of an attack that appeared for a specific cryptosystem known as TSZ. We bring in suggestion an amelioration of this system by integrating a pre-ciphering step using genetic algorithms in order to prevent the discover of texts by cryptanalyzing the old system.

Keywords: homomorphic encryption, privacy preserving, evolutionary encryption. Réf :07_09

Une nouvelle stratégie de chiffrement d'images

Assia Beloucif, Lemnouar Noui
Département d'informatique, Université de Batna, Batna, ALGERIE
Département de mathématiques, Université de Batna, Batna, ALGERIE

Abstract
In this paper, we propose a new symmetric images encryption scheme. Our algorithm creates a strong relationship between the encrypted image and the secret key in order to prevent the knowledge of the palin-image without the knowledge of the key. The proposed image encryption algorithm is based on rotations, the XOR operation and the use of companion matrices. Unlike cryptographic algorithms which based on permutations with small key spaces, the proposed image encryption algorithm has a large key space. Thus, it prevents brute force analysis. Simulation results show the effectiveness and the security of our scheme.

Mots clé: Cryptage d'image, confidentialité, sécurité, sensitivité Réf :08_11

A Novel Algorithm for Image Encryption Based on Matrix Transformation

Karima Djebaili
Department of Computer Science, University of Batna, Batna, Algeria1 Department of
Lamine Melkemi
Mathematics, University of Batna, Batna, Algeria2

Abstract
In this paper we are concerned with the problem of protecting the transmission of digital images over insecure channel. Such an encryption image system is judged efficient and secure if statistical and differential tests reveal satisfactory results and the system should design to resist cryptanalysis attacks including brute force and known/chosen plaintext attacks. On the other hand the encryption and decryption process require reasonable time and hardware space.
In this context we propose a symmetric key cryptosystem using matrix transformation and Householder reflector, which achieve the requirements related to its security and efficiency. We performed a series of tests and comparisons to confirm the efficiency of this method. Therefore, we may say that the proposed scheme has a high security and high capability to resist statistical, differential and known/chosen plaintext attacks, also this method eliminates the computational complexity involved in finding inverse of the key while decryption.

Keywords: Image encryption; matrix transformation; Householder reflector; statistical tests; differential tests.
Réf :09_12

Biometry based on retinal analysis

BOUCHERK Kahina, AMEUR Zohra
Laboratoire d'Analyse et de Modélisation desPhénomènes Aléatoires(LAMPA)
Université Mouloud Mammeri, Tizi Ouzou, Algérie
M K. Nguyen
Laboratoire Equipes de Traitement de l'Information et Systèmes (ETIS)/ENSEA
Université de Cergy-Pontoise/ CNRS UMR 8051,F-95104 Cergy-Pontoise, France

Abstract
The biometrics analysis is among powerful techniques used for people recognition. It's well adapted for high security applications. In this paper, we present a method of vascular retina network segmentation with characteristic points detection used as biometric signature. The method consists of three steps: first, enhancement of images using Gaussian filters network oriented in several directions. Second, binarisation based on entropic thresholding. In the final step, the intersection points characterizing the vascular network are extracted.

Keywords: rétine ; filtre gaussien ; crossing number ; seuillage entropique ; segmentation d'images.
Réf :10_13

Software Implementation of an extended RSA Cryptosystem based on binary exponentiation

Hentabli Wahiba
Telecommunications Department, University of science & technology Houari Boumediene
P.O.Box 32 El Alia 16111 Bab Ezzouar, Algiers,Algeria
Merazka Fatiha
Telecommunications Department, University of science & technology Houari Boumediene
P.O.Box 32 El Alia 16111 Bab Ezzouar, Algiers,Algeria

Abstract
The increasing demand of security in the communication and cryptography domain, has involves the development of a new and efficient software securitymodule which started to get the primary preference.
A software implementation of RSA encryption based on binary exponentiation under Linux platform is the purpose of our work. Using the GMP library to fast RSA algorithm under several key sizesis the best solutionperforming the Cipherfing and Deciphering process.

The RSA algorithm is the most used in public key ciphering. Since it was presented in 1977, designers have proposed several architectures and implementations to improve its performance using different techniques. It is used for Crypting and Decrypting operation involving the mathematical equation of modular exponentiation: $s=x^y \bmod m$.
The architecture, based on binary exponentiation, utilizes a MSB or LSB method as main operations for concurrent hardwired multipliers to perform crypting and decrypting operations.
Our design executesRSA algorithm for [512, 768, 1024, 1280, 1536, 1792, 2048] key-seizes in a few micro-seconds using GMP library as principal unit to accelerate the modular exponentiation.
In this paper, we present an extended RSA cryptosystem for several keys under software platform using the binary modular exponentiation and highlight the compilation results under Linux C++ platform.

Keywords: rsa; bit-length key-size; binary modular exponentiation; gmp library; C++ implementation.
Réf :11_18

Etude d'un système de cryptage basé sur le problème du mot dans un monoïde libre

Nacer GHADBANE, Douadi MIHOUBI
LMPA, Département de Mathématiques, Université de M.sila, Algérie

Résumé
Dans ce travail, on s'intéresse au protocole ATS-monoïde (P. J. Abisha, D. G. Thomas et K. G. Subramanian), l'idée de ce protocole est de transformer un système de Thue $S_1 = \langle \Sigma, T \rangle$ pour lequel le problème du mot est indécidable en un système de Thue $S_2 = \langle \Delta, T_\theta \rangle$ où $\theta \subseteq \Delta \times \Delta$ pour lequel le problème du mot est décidable en temps linéaire. Plus précisément, on donne un exemple sur cette méthode et un autre exemple sur l'algorithme Algo-ATS-monoïde pour retourner une clef équivalente à une Clef Secrète dans un protocole ATS-monoïde donné.

Mots clés: Monoïde libre, Système de Thue, Homomorphisme de monoïdes, La fermeture d.une relation binaire, Problème du mot dans un monoïde, Cryptographie à clé publique.
Réf :12_24

Etude et Implémentation Pipeline Sur FPGA de l'Algorithme de Chiffrement AES

Filali Mohamed Amine
Faculté d'électronique, Université de science et technologie Mohamed Boudiaf USTO-MB

Résumé
Les chiffrements par bloc sont largement utilisés dans le système de communications sécurisés ils sont proposés afin de d'assurer la confidentialité dans l'échange des données à travers les systèmes de communication avec des performances élevées .dans ce contexte plusieurs aspects doivent être pris en considération. En particulier. Le crypto système doit être sûr. La sécurité d'un algorithme de chiffrement par blocs est généralement vérifiée par sa résistance contre les attaques connus. Le second aspect est lie à l'implémentation de l'algorithme qui doit avoir un débit élevé.
Le travail présenté dans ce mémoire, propose une étude d'implémentation pipeline d'un algorithme de chiffrement symétrique par bloc AES combiné à un système de communication sécurisé, en temps réel en utilisant un circuit programmable FPGA de type Virtex de XILINX.
Dans ce cadre nous avons conçu une architecture pipeline de algorithme AES .la méthodologie de conception est la suivante :procéder a une implantation logiciel de cette architecture afin de pouvoir la valider .puis choisir les contraintes d'implantation sur circuit numérique et enfin aborder l'implantation matérielle proprement dite par une description comportementale de architecture à l'aide de langage VHDL .une simulation Fonctionnelle à l'aide du simulateur Model Sim et enfin une synthèse logique à l'aide de synthétiseur XST de ISE fondation 9.2i

Mots Clefs: pipeline, circuit FPGA, algorithme AES, VHDL, simulation fonctionnelle.

Réf :13_26

A New Pseudo Random Sequence Generator Based on the Chaotic System Chen

Rafik HAMZA, Faiza TITOUNA
Department of Computer Science;Faculty Sciences, University of Batna-2,
Fasdis, Batna, Algeria

Abstract
In this paper, a new pseudo random bit sequence generator based on the chaotic map chen is proposed. In this approach, we have solved the problem of non-uniform probability distribution in the chaotic system chen. Indeed, the statistical tests and the security analysis are successfully checked, which means that our approach can withstand to various attacks. We have also presented and discussed the implementation of image encryption based on the proposed algorithm. The experimental results have showed that our method is interesting for a real application on cryptography.

Keywords: Pseudo random, Probability distribution, Chaotic system chen, Encryption images.

Réf :14_27

Hyperchaos-Based Multimedia Encryption for Device-to-Device Communications

S. Benzegane, S. Sadoudi and M. Djeddou
Laboratoire Systèmes de Communications, École Militaire Polytechnique, Alger, Algérie

Abstract
In this paper, we present a software development for Hyperchaos-based video/audio streaming encryption for Device-to-Device (D2D) Communications using a hyperchaos-based Random Number Generator (HRNG) implemented in C#. The software implements and uses the proposed HRNG to generate key stream for encrypting and decrypting video and audio data in real-time. The HRNG consists of Hyperchaos Lorenz system which produces four signal outputs encryption keys of high quality randomness. The high quality of generated true random numbers is confirmed by passing standard NIST statistical tests.
Keywords: H-TRNG, Lorenz system, Hyperchaos, C#, UDP/IP. Réf :15_28

A robust watermarking scheme using a SVD technique and Differential Evolution in the algorithm of compression JPEG 2000

Razika SOUADEK, naceur-Eddine BOUKEZZOULA
LIS laboratory, Department of Electronic, University of Setif, Setif, Algeria

Abstract
A digital image watermarking algorithm using the algorithm of compression JPEG2000 (Joint Photographs Expert Group 2000),the Singular Value Decomposition technique (SVD) and Differential Evolution algorithm (DE) has Been presented. In this algorithm, we assembled all these techniques in order to give better performances. The impact of JPEG2000 on the quality of image is the reduction of the redundancy in the value of pixels; this algorithm permitted to embed the pixels of watermark image into the cover image. The purpose of SVD in the watermarking system is to increase the Impermeability and invisibility. Differential evolution algorithm used to obtain a better robustness with improved imperceptibility. In detail, we insert the watermark image in the singular value S of componentsLL3 and HL3of the third levels of DWT in the cover image of compression algorithm, the scaling factor key is calculated by DE algorithm. The discrete wavelet transform (DWT) used in the JPEG2000 compression is 2D DWTusingDaubechies 9/7 filter bank of three levels added to the phase of the quantification. The impact of compression algorithm JPEG 2000 is evaluated by using the parameters PSNR (Peak Signal to Noise Ratio) and NC (Normalized Correlation). The objective of this work has been achieved.

Keywords: watermarking image, Differential Evolution algorithm, JPEG2000 compression, Discrete Wavelet Transform, and Singular Value Decomposition.

Réf :16_29

Cryptage Basé Chaos du Signal Parole

Dalila Slimani
LISIC Lab. Telecommunications Department, USTHB University,
P.O.Box 32 El Alia 16111 Bab Ezzouar, Algiers, Algeria
FatihaMerazka
LISIC Lab.Telecommunications Department
USTHB University
P.O.Box 32 El Alia 16111 Bab Ezzouar, Algiers, Algeria
Safwan EL ASSAD
Laboratoire IETR Polytech Nantes Site de la Chantrerie Rue C. Pauc
BP 50609 44306 NANTES CEDEX 3 France

Abstract
To secure large data efficiently, chaotic encryption is a promising alternative to standard symmetrical encryption algorithms such as DES, 3DES and AES. In this paper, we proposed an encryption system for speech signals based on chaos. We use, for encryption and decryption of the speech signal, the combination of 3 chaotic maps: Logistic map, Henon map and Ikeda map. Moreover, the performance of the proposed algorithm is also estimated using the correlation coefficient quantity, the signal to noise ratio (SNR) and the Peak Signal to Noise Ratio PSNR.

Keywords: Cryptographie, chaos, signal parole Réf :17_32

Sharing secret based on MDS codes for image encryption

Noui Oussama
Department of Computer science,
Faculty of Mathematics and Informatics,University of Batna 2, Algeria
Noui Lemnouar
Department of Mathematics,
Faculty of Mathematics and Informatics, University of Batna 2, Algeria

Abstract
Data security becomes an important issue nowadays, in this paper, we propose an approach that illustrates the application of sharing secret in image encryption, we focus on secret sharing based on MDS codes. In the proposed scheme, orthogonal and permutations matrices are generated, furthermore the encryption and sharing secret are combined, this increases the level of obtained security.
The proposed scheme has a large key space enough to resist all kinds of brute force attacks, and provides a high confusion and diffusion quality which offer a security against cipher image only attack, known and chosen plain image attacks, differential and exhaustive attacks, our scheme were tested on many test images under different experiments and showed good results.

Keywords: Secret sharing, image encryption, MDS codes, confidentiality. Réf :18_34

Construction d'une Suite aléatoire par le biais de la Carte PWLCM : Application aux S-Boxes de RC4

Assia MERZOUG
Laboratoire de Codage et de la Sécurité de l'Information (LACOSI)
Université de l'Hadj Lakhdar Batna, Batna, ALGERIE
Adda ALI-PACHA, Naima HADJ-SAID
Université des Sciences et de la Technologie d'Oran Mohamed Boudiaf, USTO-MB BP 1505 El M'Naouer Oran, ALGERIE

Résume
Dans ce travail, on essaie de proposer une méthode basée sur la carte PWLCM pour la construction d'une suite aléatoire et de l'utiliser dans le flux symétrique RC4.
La nouveauté dans cette démarche, c'est la transformation de cet algorithme, en un chiffrement à clé secrète, avec une même complexité.

Mots Clés: Cryptographie, flux RC4, Carte PWLCM, suite aléatoire. Réf :19_20

Implémentation sur un circuit FPGA du Générateur Blum-Blum-Shub en vue de son application à la Cryptographie

Hasni BENDOUMA, Adda ALI-PACHA, Naima HADJ-SAID
Laboratoire de Codage et de la Sécurité de l'Information
Université des Sciences et de la Technologied'Oran USTO, Mohamed Boudiaf
BP1505 El M'Naouer Oran 31000 ALGERIE

Résume
Vu qu'il est difficile d'obtenir de « vrais » nombres aléatoires et que, dans certaines situations, il est possible d'utiliser des nombres pseudo-aléatoires, en lieu et place de vrais nombres aléatoires par des générateurs particulièrement adaptés à une implantation informatique, donc plus facilement et plus efficacement utilisables. La plupart des algorithmes pseudo-aléatoires essaient de produire des sorties qui sont uniformément distribuées et présentant certaines propriétés du hasard.
Certains générateurs pseudo-aléatoires sont dits *cryptographiques sûrs* quand certaines contraintes sont satisfaites, c'est le cas du générateur **Blum Blum Shub** qu'on va l'étudier et l'implémenter sur un circuit FPGA.
Mots Clés: Blum Blum Shub, stream-ciphers, Cryptographie, analyse statistique. Réf :20_25

FPGA design and Implementation of Histogram Algorithm for image processing

KHITAS Mehdi1, ZIET Lancene2 and RADJAH Fayçal
Electronics department technology faculty L.C.C.N.S Laboratory Setif-1 University Setif,
Setif, Algeria

Abstract
In this article, we propose a hardware implementation for calculating the histogram algorithm. This module receives information as a data stream from an SPI bus interfacing SD-CARD, all the devises are controlled by a system based on NIOS II. The design is validated on Altera DE1-prototyping board.

Keywords: histogram analysis; NIOS II processor; Qsys builder; SD card. Réf :21_37

3D Partial Face Recognition using Local Descriptors

Samia Bentaieb, Abdelaziz Ouamri
Signals and Images Laboratory
University of USTOMB
Oran, Algeria

Abstract
In this paper, we propose and evaluate a 3D face recognition approach using Speeded Up Robust Feature algorithm (SURF) on range images under pose variations and presence of occlusions. First 3D scans are preprocessed then SURF is used on shape index maps to find interest points and their descriptors. Similarity between gallery and probe faces is evaluated by combining the number of matching keypoints and the Euclidean distance between their coordinates. The feasibility of using SURF on the shape index map for face identification is presented through experimental investigation conducted on Bosphorus database. It achieves rank one recognition rates of 98.35, 96.85 and 98.18% on pose, occlusion, and both subsets, respectively.

Keywords: 3D face recognition, SURF, Shape index, Pose, Occlusion. Réf :22_38

A Fragile watermark based on shortened BCH (16,11) for n out of n secret sharing scheme

Nour El Houda Asma MERABET
University of Batna, Batna, Algeria
Redha BENZID
University of Batna, Batna, Algeria

Abstract
Secret sharing is a cryptography technique aims to share and encrypt multimedia data in such a way that the decryption process can be done by human visual system. Like all the others techniques of cryptography, sending data over internet can be menaced either by the attacks of hackers or by the noise caused by the transmission channel. In this paper we enhance the security of one of the perfect secret sharing scheme that overcomes the main drawback of traditional visual cryptography with simple XOR operation in the decryption process, by using a fragile watermark based on shortened BCH (16, 11) to detect and correct potential errors.

Keywords: secret sharing scheme; watermark; shortened BCH error correction. Réf :23_39

Algorithme de Cryptage Symétrie pour les Données Multimédias Utilisant OEP

Yakouta Zarouk
LabSTIC, Université 8 mai 1945
Guelma, Algérie
Ismahane Souici
LabSTIC, Université 8 mai 1945
Guelma, Algérie
Hamid Seridi
LabSTIC, Université 8 mai 1945
Guelma, Algérie

Résumé
Le développement des communications et les transmissions numérique ont poussé le cryptage des données à se développer rapidement afin de protéger l'information contre n'importe qu'elle piratage ou utilisation malveillante. Dans ce travail, on va proposer un algorithme de chiffrement des donné multimédias basé la génération de deux clés symétriques en utilisant un algorithme d'optimisation par essaim de particules OEP. Ces deux clé seront utilisées à la permutation des lignes et colonnes dans le but de diffuser les pixels d'image. Pour renforcé la résistance du l'algorithme aux attaque statistique une confusion des pixels est effectuée par l'opération OU exclusive. Des résultats et discussions sont présentés dans ce papier afin de montrer l'efficacité du schéma proposé.

Mots clé: algorithme de cryptage, sécurisation des multimédias, cryptage d'image, cryptage sélectif.

Réf :24_42

Application de la Transformée de Fourier pour la sécurité des images

Benmessaoud Nabila, Adda Ali Pacha, Hadj Said Naima
Département d'Électronique
Université des Sciences et de la Technologie d'Oran, USTO- BP. 1505 Oran El M'naouer
Oran, Algerie

Résumé
La sécurisation des informations est un thème de recherche pour lequel on assiste actuellement à un fort regain d'intérêt, principalement pour deux raisons. C'est d'une part une conséquence du formidable développement des télécommunications des les trente dernières années. La révolution numérique a engendré des moyens plus faciles pour le traitement, le stockage et la transmission des images numériques. Cependant elle a aussi engendré des moyens de falsification, de contrefaçons et d'espionnage très avancés. Le risque est encore plus grand dans un environnement ouvert tel que la transmission des images satellitaires au sol. Dans cet article nous allons proposer une approche pour le cryptage des images en introduisant la transformée de Fourier discrète ainsi que le signal chaotique pour arriver à construire une suite de coefficients aléatoires qui seront par suite utilisés pour le cryptage de différentes images.

Mots Clés : Transformée de Fourier discrète, Cryptage, Les systèmes chaotiques, suite aléatoire.

Réf :25_43

Le Chiffrement par Blocs à Base du Chaos: un Aperçu

I.TALBI&S. BOUGHABA
Université Mentouri -Constantine-, Algérie.

Résumé
Une variété de cryptosystèmes chaotiques a été étudiée au cours de la dernière décennie. La plupart d'entre eux sont basés sur la structure de Fridrich, qui est basée sur l'architecture traditionnelle de confusion et diffusion proposée par Shannon.

Comparés avec les cryptosystèmes traditionnels qui sont: (DES, 3DES.AES.etc.), les cryptosystèmes basés sur les chaos sont plus flexibles, plus modulaires et faciles à implémenter, ce qui les rend plus appropriés pour le chiffrement de données à grandes échelle telles que les images et les vidéos. Le cœur de n'importe quel cryptosystème à base chaotique est le générateur chaotique. Une partie de l'efficacité du système (robustesse, rapidité) dépend généralement de lui (c.à.d. le générateur chaotique).

Dans cet exposé, on donne un aperçu de l'état de l'art de chiffrement par blocs en utilisant le chaos, et nous décrivons certains de nos régimes déjà proposés.

Aussi, nous allons nous concentrer sur les caractéristiques essentielles du générateur chaotique numérique qui a été publié en Octobre 2011 comme un brevet français et également en 2013 une extension du brevet en Europe, en Chine, Japon et USA a été publiée. La performance nécessaire d'un bloc de chiffrement basé sur le chaos, en termes de niveau de sécurité et la vitesse du calcul dépend de l'application considérée. Il existe un compromis entre la sécurité et la vitesse de calcul. La sécurité de ces blocs de chiffrement sera analysée.

Mots clés: Cryptosystèmes à base chaotique, générateur chaotique numérique, analyse de sécurité.
Réf :26_44

Strong Genetic Stream Cipher Design to Secure Mobile Phone Telepony

Ghazli Abdelkader, Hadj Said Naima, Alipacha Adda
Faculty of Sciences, University of Sciences and Technology Oran, Algeria
Ghazli Boubakeur
Faculty of Technology, Tahri Mohamed University Bechar, Algeria

Abstract
Mobile phones are considered to be the most common communication devices in history. Recently, mobile phones are not only used for communication but also, to sending and receiving important data such as, social security numbers, bank account details and passwords. The global system for mobile communications GSM uses the encryption algorithms collectively called as A5 families which are a symmetric-key Stream ciphers that generate pseudo-random binary sequences which are used to encrypt the message signals on bit-by-bit basis. However, these algorithms suffer from a lot cryptanalysis. In this paper, we propose new genetic pseudo random bit generator (PRBG) based on genetic algorithm to make GSM encryption algorithm A5 robust and resistive to the attacks such as time memory trade off, divide and conquer. A basic security analysis shows that the proposed algorithm is more resisters for cryptanalysis with a good quality of bits stream produced by our generator called genetic A5.
Keywords: GSM; security; genetic; stream cipher; LFSR
Réf :27_45

CryptoPage: vers la fin du piratage informatique?

Wassila Issaadi
Electrical Engineering laboratory, Faculty of Technology,
University of Bejaïa, 06000 Bejaia, Algeria.

Résumé
Afin d'aider à résoudre les problèmes de piratage informatique et les besoins de confidentialité dans les applications et les communications modernes, cet article présente une technique matérielle permettant de rajouter du chiffrement fort à un processeur. Ce mécanisme associé aux caches et à la gestion mémoire permet de chiffrer les instructions du programme ainsi que les données en mémoire pour assurer une bonne résistance aux attaques sur le bus du microprocesseur. Cela permet de concevoir par exemple des programmes capables de ne tourner *que* sur une seule machine au monde, assurant ainsi la confidentialité de l'application et des communications. Réf :28_46

Vers l'Implémentation d'un Modèle de Contrôle d'Accès pour les Systèmes d'Informations en Santé

Belaidi Asma, Abderrahim Mohammed El Amine
Laboratoire de Génie Biomédicale, Université de Tlemcen

Résumé
L'accessibilité aux ressources d'information dans les systèmes de santé est un aspect très important. Ce travail de recherche porte sur la protection des données médicales et s'est centré sur le contrôle d'accès dans les systèmes d'information en santé et plus spécifiquement sur les modèles de contrôle d'accès. Dans cet article nous avons dressé un état de l'art des différents modèles de contrôle d'accès. La comparaison entre ces modèles nous a permis de proposer un modèle répandant aux exigences du domaine de la santé.

Mots clé : Contrôle d'accès, DAC, MAC, RBAC, TBAC, TMAC, Or-BAC Réf :29_35

Situated Work Analysis of Attribute-Based Encryption (ABE): Case of Healthcare

Souad SELMANE
Département d'informatique
Laboratoire LAMIE
Batna, Algérie
Abdelmadjid ZIDANI
Département d'informatique
Laboratoire LaSTIC
Batna, Algérie

Abstract
In these recent years, we are witnessing more and more significant advances of computing technologies, particularly through their increasing use in the health area which constitute the main concern of this paper. Indeed, healthcare implies not only managing access to sensible patients' information but also allow sharing it to enable collaboration among physicians teams. We are thus faced with the dilemma of facilitating accesses on the one hand, and preserving patients' personal information that can be threatened by spies (use, misuse, disclosure, destruction, modification, and counterfeit, etc.) on the other hand. The main purpose of this paper is to provide an analysis focused

on securing Patients' Electronic Health Records (EHR) accesses and sharing. We plan to explore the Attribute-Based Encryption (ABE) method which seems to be the most appropriated one. We firstly introduce EHR concept to explicitly show its content sensibility and highlight the related security needs. The following sections outline the main ABE encryption used schemes. We discuss then, our proposed sharing model that still under study and attempted to motivate its relevance as a solution taking into account the collaboration side. Finally, we conclude our paper by specifying the opportunities opening up to our research work.

Keywords: Collaboration, access, share, EHR, ABE, sharing model. Réf :30_36

A New Robust Hybrid Transmission Scheme based on the Synchronization of Discrete-Time Chaotic Systems

Ouerdia Megherbi, Sarah Kassim, Hamid Hamiche, Saïd Djennoune
L2CSP-University of Mouloud Mammeri
Tizi-Ouzou, Algeria
Maâmar Bettayeb
University of Sharjah
Sharjah, UAE

Abstract
In this paper, we propose a new robust hybrid data transmission scheme based on discrete-time chaotic systems. The transmitter is composed of two different discrete-time chaotic systems: the Lozi and the fractional-order modified-Henon maps. In order to increase the robustness of the transmission scheme, one of the Lozi system states is used to encrypt the original message signal. The obtained encrypted message is introduced in the dynamics of the fractional-order modified-Henon system. The fractional derivative orders are considered as additional secret keys, which enhance furthermore the scheme security. The receiver consists of two discrete-time observers: an impulsive observer and a delayed fractional-order observer. Once the synchronization is established between the transmitter and the receiver, the message can be recovered at the receiver end.

Keywords: Secure communication, Chaotic systems, Impulsive synchronization, Discrete observer, Modified-Henon map, Lozi map, Fractional-order systems. Réf :31_05

A novel robust image transmission scheme based on fractional-order discrete chaotic systems

Sarah Kassim, Hamid Hamiche, Said Djennoune
Department of Control Engineering
L2CSP, UMMTO
Tizi-Ouzou , Algeria

Abstract
In this paper, a new image transmission scheme based on fractional discrete-time chaotic system is presented. The transmission scheme consists of a fractional-order modified Henon map considered as transmitter and a delayed step-by-step observer used as receiver. The transmitter parameters and fractional orders play the role of secret keys of the transmission scheme. To increase the robustness of the secure image transmission, the message to send is firstly encrypted by an encryption function then inserted by inclusion method in the chaotic discrete time system dynamics. Simulation results are presented to highlight the performances of the proposed method.

Keywords: Private communications, Image encryption, Fractional-order systems, Modified-Henon map, Step-by-step observer, Robustness. Réf :32_06

AUTHENTIFICATION BIOMETRIQUE

Toumi Assia, Adjoudj Réda
Department of Computer Science, Sidi Bel-Abbes University, Algeria
Toumi Tarek
Department of Computer Science, Batna University, Algeria

RESUME
Avec l'évolution de la puissance des ordinateurs et la diversité des transactions d'échange et de communication, les moyens de sécurité traditionnels comme les mots de passe ne sont plus fiable, et ils ont devenu une cible facile à l'usurpation par les malveillants, pour ces raisons on a fait appel à la biométrie pour résoudre ce problème grâce à l'utilisation des caractéristiques spécifiques à chaque être humain comme : le visage, la voix, l'empreinte digital, l'iris, la géométrie de la main et même la démarche de la personne, car elles ne peuvent pas être falsifiées ou usurpées sans qu'elles ne seront repérées. Suite à ces raisons une brève introduction à la biométrie avec quelques modalités biométriques utilisées dans l'authentification personnelle des utilisateurs est présentée.

KEYWORDS: Biométrie, Modalités, Sécurité. Réf :33_22

The relation between counting primes and twin primes

Islem Ghaffor
Department of Mathematics, USTO-MB

Abstract
In this paper we give a new formula for the relation between counting primes and twin primes, we use in this formula the arithmetic progressions and the cardinal of the set.

Key words: Prime-counting function, twin prime conjecture, the cardinal of the set. Réf :34_02

Repeated-Root Constacyclic Codes over Finite Fields

Aicha Batoul, Kenza Guenda and T. Aaron Gulliver

Abstract
In this paper we investigate the structure of repeated root constacyclic codes of length $2ampr$ over Fps with $a \geq 1$ and $(m; p) = 1$. We characterize the codes in terms of their generator polynomials.This provides simple conditions on the existence of self-dual negacyclic codes.Further, we gave cases where the constacyclic codes are equivalent to cyclic codes.

Keywords: Repeated-root Constacyclic codes, Negacyclic Codes, Self-dual Codes. Réf :35_21

Some Results on Permutation Polynomials over Finite Fields

Nouara Zoubir and Kenza Guenda
USTHB, Laboratory of Algebra and number theory, BP 32 El Alia, Bab Ezzouar, Algeria

Abstract
Permutation polynomials are an interesting subject of mathematics and have applications in other areas of mathematics and engineering. In this paper, we give several classes of complete permutation polynomials over finite fields.

Réf :36_47

A new meta-heuristics for Intrusion Detection System by scenario inspired from the protection system of social bees

Mohamed Amine Boudia, Reda Mohamed Hamou, Ahmed Chaouki Lokbani,
Abdelmalek Amine and Amine Rahmani
University of Saida, Algeria

Abstract
In this paper, we will propose a meta-heuristic for intrusion detection system by scenario, inspired from the protection system of social bees to their hive. This approach is based on a specialized multi agent system where we will give a limited responsibility to each guard bee agent : to secure only one port, this specialization aims to better exploit the training set and the hardware and software performance. we will start this paper by a short introduction where we will see the importance of IT security especially today, then we will give a little insight into the state of the art, before starting the essential part of a scientific paper: "our approach" where we will explain the natural model, and then we'll simplified our model in a modelling table to share our vision and philosophy to switch from natural model to artificial model, and then we will detail the artificial model we are going to experience in the next chapter, we will discuss the results and make comparison in the two following chapter to get out with a conclusion and perspective of our future work.

Keywords: social bees, intrusion detection system, IT Security, scenario approach, kddcup'99, Réf :37_10

Negacyclic Codes Over $Z4 + u Z_4 + u^2 Z_4$

Nouara Mokhtari,
faculty of science, department of mathematics UMBB, University of Boumerdes, Algeria
Aini Laoudi
Faculty of Mathematics USTHB, University of Science and Technology of Algiers, Algeria

Abstract
In this paper we study negacyclic codes over the ring $R = Z_4 + uZ_4 + u_2Z_4$, $u_3 = 0$. We consider negacyclic codes of odd length, and we give their complete structures. A necessary and sufficient condition for these negacyclic codes to be free is given. Then, we discussed a repeated root negacyclic codes of length 2^k. Finally, the existence of self dual codes over R are discussed. Réf :38_17

A new Trust framework for Wireless sensor networks based Internet of things (TWI)

Ouassila HOCEINI
LARI Laboratory
Mouloud Mammeri University, Tizi Ouzou, Algeria

Abstract
With the emergence of WSN (wireless sensor networks) and new technologies such as RFIDs, sensors, actuators, cloud computing and their green (smart) applications make cities smart and provide the opportunity to collect and effectively use large scale city data for information awareness and decision making. Moreover, in parallel with the increasing autonomy of objects to sense and react on the environment, IoT (Internet of Things) and WSN security should move towards a greater autonomy in perceiving threats and reacting to attacks. In this work, we proposed a trust framework in order to detect and revoke compromising nodes from IoT environment and overcome several security issues in WSN based IoT. Simulation results show that TWI detects selfish and defective objects and prevent us of insider attacks. Réf :39_16

New Private Information Retrieval using combination of filters based social workers bees' algorithm

Hadj Ahmed BOUARARA, Mohamed Reda HAMOU, Abdelmalek AMINE
GeCoDe Laboratory, Department of Computer Science
Tahar Moulay University of Saida Algeria

Abstract
Recently, a novel form of web services had seen the light under the name of Cloud Computing which presents the dematerialisation of software, systems and infrastructures basing on virtualization techniques. However, in a world where digital information is everywhere, recent researches proved that 90% of the information existed on the web was created in the last few years, finding the desired information has become a crucial problem. In other hand, the users of cloud services starting asking about their privacy protection, particularly when they lose control of their data during the treatment and even some of them think about counting the service providers themselves as honest attackers. For that, new approaches and ideas had been published in every axis of the privacy preserving domain. One of these axis consists of a special retrieval models which allow both finding and hiding sensitive desired information at the same time. The substance of our work is a new system of private information retrieval protocol (PIR) composed of four steps the authentication to ensure the identification of authorised users. The encryption of stored documents by the server using the boosting algorithm based on the life of bees and multi-filter cryptosystems. The information retrieval step using a combination of distances by social bees based on the principle of filtering where a document must pass through three filters controlled with three types of worker bees, the bee queen represents the query and the hive represents the class of relevant documents. Finally a visualization step that permits the presentation of the results in graphical format understandable by humans as a 3D cube. Our objectives is to amend the response to users' demands.

Keywords: Private Information Retrieval, Visualisation, Social bees, Boosting Cryptosystem, Cloud Computing.
Réf :40_17

Motion detection based motion saliency detection

Karima Ait Saadi and Bahia Yahya-Zoubir
Centre de Développement des Technologies Avancées (CDTA)
Division Télécom

Abstract
The human visual system has the ability to locate a moving object in a visual scene rapidly. Modeling this human behavior is still a big computational challenge. In the area of computational vision systems saliency detection is a promising approach because it determines the most relevant objects of a given scene using a human-inspired way. In this paper a novel motion saliency detection method is presented, the proposed method uses the optical flow to generate the motion saliency map. Once the motion saliency map is obtained a refining stage is performed to eliminate unnecessary details. The performances of the pro-posed method were experimented on the publicly available BMC database and the obtained results are satisfying.

Keywords: Saliency map; optical flow; motion; visual attention; scene analysis.
Réf :41_33

Conditional Privacy Preservation for VANET Safety Applications

Ines Khacheba, Mohamed Bachir Yagoubi
Laboratory of Computer Science and Mathematics University of Laghouat,
Laghouat, Algeria

Abstract
Vehicular Ad Hoc Network (VANET) is a promising vehicular communication system, which offers a wide range of applications and services for the purpose of improving road safety, and traffic management. However, it faces many security and privacy issues, especially for location privacy. Indeed, if the vehicles' location privacy can't be protected, drivers won't accept the VANET. To protect vehicles' location privacy, the VANET should use privacy preservation schemes. However, a malicious vehicle can't be tracked and identified if a complete privacy preservation scheme is used. Therefore, a conditional privacy preservation scheme should be employed to secure VANET systems, where a Trusted Authority (TA) has the ability to reveal and revoke a malicious vehicle's real identity. This is known as conditional tracking. Unlinkable pseudonyms schemes can build conditional privacy preservation. In this study, we address the problem of achieving location privacy to secure VANET systems. We look for how to generate pseudonyms, and introduce an effective Pseudonyms Generation Protocol (PGP), in order to support the conditional tracking, and thus to achieve the requirement of conditional privacy preservation.

Keywords: Vehicular Ad Hoc Networks, Location Privacy, Conditional Privacy Preservation, Pseudonyms Generation, Connection Card, Conditional Tracking

Réf :42_23

Schéma de contrôle d'accès aux données médicales dans les systèmes e-santé basé sur le TOTP

MIROUD Mohammed El Mustapha
Laboratoire LAMOSI, Département d'Informatique,
Faculté des Mathématiques et Informatique, USTOMB, 31000 Oran, Algérie
BELKADI Khaled
Laboratoire LAMOSI, Département d'Informatique,
Faculté des Mathématiques et Informatique, USTOMB,
31000 Oran, Algérie

Abstract
Dans cet article nous présentons un modèle de contrôle d'accès aux dossiers médicaux des patients stockés dans des systèmes d'e-santé. Le modèle que nous proposons est basé sur le HMAC Time Based One Time Password que nous utilisons comme Token distribué par le patient aux professionnels de santé pour que ceux-ci puissent accéder à son dossier. Notre modèle est également basé sur le chiffrement total du dossier, ce chiffrement est effectué à l'aide de l'algorithme AES, cependant afin d'optimiser les performances du système, étant donné qu'un chiffrement total va influer négativement sur celles-ci, nous avons donné au patient la possibilité de catégoriser ses données selon trois catégories de sensibilité, chaque catégorie sera chiffrée avec une taille de clé proportionnelle au degré de sensibilité que lui aura attribué le patient.

Keywords: E-santé, HMAC TOTP, Contrôle d'accès, AES, Dossiers Médicaux, Sécurité. Réf :43_48

Keynotes

The promising future of chaos theory for Personal Cryptographic Security

René Lozi

The first example of the use of chaos for cryptographic purpose goes back to the early 90' when Pecora and Carroll [1] found how to synchronize chaotic systems of differential equations. A first reported experimental secure communication system via chaotic synchronization was built two years after [2], using the electronic Chua's circuit and was soon improved reducing the noise of the transmitted signal [3].
Since this pioneer works, the possibility for self-synchronization of chaotic oscillations has sparked an avalanche of researches on application of chaos in cryptography.
Nowadays, twenty-five years after the beginning of chaotic cryptography this research field continues to be active, as shown by the large number of papers being published and it is thriving in form of new and interesting proposals in all areas of modern cryptology. Some patents have been also taken out.
However in spite of the momentum given by these researches, chaos-based cryptography does not yet gain advantage against traditional techniques like AES or RSA because most of the authors are still using chaotic mappings initially discovered long time ago. Nonetheless several improvements have been recently done in chaos theory, allowing to master completely the use of chaos in various industrial projects.
Henceforth, it seems that the spitting point were chaos-based cryptography surpasses traditional techniques will be reached in the not too distant future. It is why we think that the use of chaos theory for Personal Cryptography Security (PCS) has a promising future. In this seminar we discuss about the fascinating perspectives of this research field.

[1] L. Pecora and T. Carroll, "Synchronization in chaotic systems," Phys. Rev. Lett., vol. 64, pp. 821-823, 1990.
[2] Lj. Kocarev, K. S. Halle, K. Eckert and L. O. Chua, "Experimental demonstration of secure communication via chaotic synchronization," Int. J. of Bifurcation and Chaos, vol. 2, no 3, pp. 709-713, 1992.
[3] R. Lozi and L. O. Chua, "Secure communications via chaotic synchronization II: noise reduction by cascading two identical receivers," Int. J. of Bifurcation and Chaos, vol. 3, no 5, pp. 1319-1325, 1993.
[4] Oleg Garasym, Ina Taralova and René Lozi, "Application of observer-based chaotic synchronization and identifiability to the original CSK Model for secure information transmission", Indian Journal of Industrial and Applied Mathematics, Vol. 6, Issue 1, January-June 2015, pp. 1-26.

René Lozi professeur des universités de classe exceptionnelle a effectué l'ensemble de sa carrière à Nice. Etudiant, il a suivi les cours de J. A. Dieudonné en 1970. Après sa thèse de 3ème cycle dédiée à l'analyse numérique des bifurcations en 1975, il a été recruté au CNRS jusqu'à ce qu'il soit nommé professeur en 1991. René Thom (médaillé Fields) a été rapporteur de sa thèse d'Etat en 1983 et de son HDR (nouvellement créée) en 1987. En 1977 il s'est intéressé aux systèmes dynamiques et a publié le premier exemple explicite d'attracteur étrange (actuellement connu sous le nom de « Lozi map »).
Ses recherches portent sur l'application des systèmes dynamiques chaotiques à différents domaines : cryptographie, algorithmes génétiques, génération de nombres pseudo-aléatoires, théorie de la complexité. Depuis deux ans il étudie les propriétés des composants électroniques à mémoire (memristor) avec le Professeur Leon O. Chua (Université de Californie, Berkeley) inventeur du concept, dans le Laboratoire J. A. Dieudonné.
Il a reçu le prix annuel (créé en 2001) Dr. Zakir Husain Award 2012 de l'Indian Society of Industrial and Applied Mathematics (ISIAM affiliée aux SIAM des autres pays) en Janvier 2015 à l'université du Punjab à Patiala, pour ses travaux et son aide à la création en 1990 de cette société. Il est régulièrement « keynote speaker » dans de nombreux congrès dans de plusieurs pays.
Il s'intéresse également depuis 40 ans à la formation des enseignants (il a été Directeur de l'IREM, puis de l'IUFM de Nice en 2001-2006 et Vice-Président de l'assemblée des Directeurs d'IUFM en 2004-2006), à la didactique des mathématiques et au nouveau concept de l'Interdidactique au sein du laboratoire I3DL.

Quelques éléments de la théorie du contrôle utiles pour la récupération et la transmission de l'information

J-P Barbot

Dans cette présentation nous illustrerons l'utilité des concepts tels que l'observabilités, les singularités d'observabilités, la stabilité, … sur des exemples issues de la transmission de l'information. Ainsi, la transmission sécurisée des données sera vue du point de vue de l'observabilité. De même, dans un problème d'inversion à gauche statique sous mesures clairsemées 'compressive sensing' la construction de matrices spécifiques sera faite de façon déterministe. La reconstruction dynamique des données sous mesures clairsemées sera elle abordée du point de vue de la synthèse d'observateurs…

J-P Barbot, Professeur des Universités Classe Exceptionnelle.

Spécialités

Automatique : Système non linéaire, Observateur, mode glissant, forme normale, inversion à gauche, Système dynamique Hybride, Chaos, Compressive Sensing, Event trigger,…

Titres et diplômes :

Titres :

- Professeur des Universités à l'ENSEA (Depuis septembre 1998)
- Directeur du laboratoire Quartz EA 7393 (depuis le 7 mai 2015)
- Directeur du laboratoire ECS-Lab (ex-ECS) EA 3649 (de juillet 1999 à février 2013)
- Directeur adjoint du laboratoire ECS-Lab (ex-ECS) EA 3649 (de février 2013 au 7 mai 2015)
- VisitingProfessor à la NorthumbriaUniversity (D'octobre 2007 à 2010, renouvelé de 2010-2013)
- Membre de l'EPI- Non-A (ex ALIEN) INRIA (Depuis octobre 2006)

b-Diplômes :

1997 - Habilitation à diriger des recherches, titre : *Etude structurelle de quelques systèmes non linéaires*. Jury, Rapporteurs : A.J. Fossard, G. Bornard, A. Razek. Examinateurs D. Normand-Cyrot, N. M'Sirdi, J-P. Quadrat, Invités : S. Monaco et J-L. Thomas.

1989 - Doctorat de l'université de Paris XI, Orsay, titre *: Méthodes de calcul appliquées aux systèmes non linéaires sous échantillonnage*. Jury, Rapporteurs : S. Monaco et D. Claude, Examinateurs P. Bertrand, J-P. Louis, Directrice de thèse : D. Normand-Cyrot.

1986 -DEA d'Automatique et Traitement du Signal, Université de Paris Sud, Orsay

1985 -Agrégation de Génie Electrique

Informations complémentaires :

- Encadrement de 31 thèses soutenues et de 3 en cours (bénéficiaire de la PEDR).
- Auteurs ou co-auteurs de : 66 articles dans des revues internationales, 8 articles dans des revues nationales, 20 chapitres de livre, 191 articles de congrès 2 brevets et co-éditeur de deux livres.
- Nombre d'articles cités 254, nombre de citations 3790, h-number 30 (sourcehttps://scholar.google.com/citations?user=MKZlpIUAAAAJ le 16/02/2016)
- Membre de l'IPC de l'IFAC NOLCOS 2016, co-organisateur avec Gildas Besançon de deux sessions invités.
- Membre de l'IPC de l'IFAC Chaos 2015, Chairman de la plénière du professeur Xuanrong Chen
- IPC Chair de VSS 2014, Nantes
- IPC Co-Chair de EFEA 2014, Paris (Saint Ouen)
- Editeur associé pour IEEE TCAS 2 de décembre 2006 à janvier 2010.
- Membre du jury de l'agrégation externe de génie électrique de 2006 à 2009, auteur de l'épreuve écrite d'Automatique 2009.

- Coprésident ou vise président des congrès internationaux Chaos 06 et 09
- Coorganisateur de journées nationales : Ecole d'été, JDMACS, journées Automatique et chaos, Journée systèmes fractionnaires & contrôle de systèmes biologiques…
- Instigateur et responsable avec B. Cherki et M Djeami du master Control des Processus à l'université de Tlemcen, Algérie sous le patronage du HCFAUR.
- Membre nommé du CNU 61ème section de 1995-1998.
- Membre du comité de direction du GDR Automatique 2002 à 2005.
- Participation à de nombreuses collaborations industrielles : Alstom (control et observation d'une machine asynchrone), Sherpa (Commande d'une Pile à Combustible), GS maintenances (Commande sans capteur mécanique d'une machine asynchrone), Mov'eo Projet O2M (pré dimensionnement en mécatronique 139 K€ pour ECS-Lab), Astech et System@tic Projet Agregation (Aide à la synthèse de loi de commande 100 K€ pour ECS-Lab) et de nombreux stages de fin d'étude ingénieur en partenariat avec des industriels.
- Membre du TC 2.3 Non-Linear Control system de l'IFAC depuis 2005.
- Responsable du GT Sync commun au GDR MACS et DYCOEC I (Fin de DYCOEC I en 2013) et par le passé du GT Commande des Entraînement Electrique CEE pour le GDR Automatique.

Participation à 2 PEPS : A2SDC (Automatique et Analyse de Systèmes à Dynamique Chaotique) etGESE (Gestion Echantillonnée des Systèmes Energétiques).

Chaos-based- Information Hiding and Security: an emergent technology

Safwan El Assad
Ecole polyethnique de l'université de Nantes, Rue Christian Pauc CS 50609 Nantes Cedex 3, France.
IETR UMR CNRS 6164; Image team - site of Nantes

Security and confidentiality of image and video data is an important research topic and have been widely investigated by using standard cryptography and chaos-based cryptography. Indeed, a variety of chaos-based cryptosystems have been investigated during the last decade. Most of them are based on the structure of Fridrich, which is based on the traditional confusion-diffusion architecture proposed by Shannon. Compared with traditional cryptography, the chaos-based cryptography are more flexible which make them more suitable for large scale-data encryption, such as images and video.The heart of any chaos-based cryptosystem is the chaotic generator and so, a part of the efficiency (robustness, speed) of the system depends greatly on it. Furthermore, in stream ciphers all the security depend on the used pseudo-random number generator (PRNG).

In this talk, first, we describe threeof our chaos-based cryptosystems: two blocks ciphers and one selective stream cipher for HEVC coder at CABAC level. Then, we describe the structure of the proposed generator of discrete chaotic samples and we compare its performance (robustness, speed) with the traditional pseudo-random number generators used in standard cryptography (eStream).

Safwan El Assad received his PhD degree in electrical engineering from the University of Lille 1, France in 1987. His doctoral thesis was on electromagnetic compatibility. He joined the University of Nantes, France in September 1987, where he is now an Associate Professor. From 1988 to 1996, his main area of research was in radar imaging, remote sensing, signal and images processing. From 1996 until 2002, he developed topics in digital communications, adaptive equalization for digital channels by neural network, and e-learning. His current research area is focus on chaos-based information hiding and security including: Chaos-based crypto and crypto-compression systems for images and videos; chaos-based watermarking and stegangraphy systems. He has supervised 11 PhDs (Current 3) and 23 Master students. He worked on 4 European projects and he published (as an author, co-author) more than 150 papers in refereed international journals and conference proceedings, as well as books and 3 patents.

Applications: Transactions Security, IP security over satellite DVB, UMTS security, UWB security, WIFI security, wireless network security, copyright, data integrity, etc.

Safwan El Assad
IETR Laboratory
Institut d'Electronique et des Télécommunications de Rennes
IETR UMR CNRS 6164; Image team - site of Nantes
Ecole Polytechnique de l'université de Nantes.
Site de la Chantrerie -Rue Christian Pauc, B.P 50609
44306 NANTES CEDEX 3 - France
Tel + 33 2 40 68 30 36 ; Mobile + 33 6 76 32 28 36
Fax + 33 2 40 68 32 32
Email : safwan.elassad@univ-nantes.fr

Efficient Methods for Lattice-based Cryptography

Sedat Akleylek
Department of Computer Engineering, Ondokuz May_s University
Samsun, Turkey

In this talk, we focus on the modular polynomial multiplication the core part of the ring variant of lattice-based cryptographic schemes in terms of efficiency. We modify well-known algorithms for sparse polynomial multiplication. With the modified methods, we significantly speed up the multiplication operation over the quotient ring (Z=qZ)=(xn _ 1) in software. Then, we discuss the prime selection yielding efficient modular reduction in lattice-based cryptographic schemes. Compared with the state of the art, we obtain the lowest arithmetic complexity with the proposed list of primes for hardware implementations.

Short Biography: Sedat Akleylek received the B.Sc. degree in Mathematics majored in Computer Science from Ege University in 2004 in Izmir, Turkey, M.Sc. and Ph.D. degrees in Cryptography from Middle East Technical University in 2008 and 2010, in Ankara, Turkey, respectively. He was post-doctoral researcher at TU Darmstadt, Germany between 2014 and 2015. He is currently an associate professor at the Department of Computer Engineering, OndokuzMayis University, Samsun, Turkey. His research interests include in the areas of (post-quantum) cryptography, algorithms and architectures for computations in finite fields, applied cryptography for cyber security.

Philippe Guillot

Situation actuelle :

Maitre de conférences à l'université Paris 8
Chercheur au Laboratoire Analyse Géométrie Applications (LAGA UMR CNRS 7539)
E-mail : philippe.guillot@univ-paris8.fr
Adresse professionnelle : 2 rue de la Liberté, 93526 Saint-Denis CEDEX

Cursus

Depuis 2003	Maître de conférences à l'université Paris 8.
	Chercheur au LAGA, Equipe Protection de l'Information et Image.
2001-2003	Responsable cryptologie à Canal+ Technologies.
1999	Thèse de doctorat : Fonctions courbes binaires et transformation de Möbius.
1990-2001	Ingénieur d'étude à Thomson-CSF
1988	Agrégation de mathématiques.
	DEA Statistiques, probabilités et informatique, université de Rouen.
1982-1990	Professeur de mathématiques dans le secondaire.

Co-encadrement de thèse :

- Sabine Leveiller (ENST Paris {THALES COMMUNICATIONS) Quelques algorithmes de cryptanalyse du registre filtré Soutenue le 23 janvier 2004.
- Florent Bernard (Université Paris 8 {THALES COMMUNICATIONS) _Etude des algorithmes arithmétiques et leur implémentation matérielle. Soutenue le 15 octobre 2007.
- _Jérémy Parriaux (Université de Lorraine) Contrôle, synchronisation et chiffrement. Soutenue le 3 octobre 2012.

Activités de recherche. Méthodes algorithmiques et algébriques de la cryptographie symétrique et asymétrique (4 ouvrages, 5 articles dans des revues, 15 articles scientifiques divers)

- Fonctions booléennes, étude des critères, construction, évaluation.
- Attaques par canaux cachés sur les implémentations, carte à puce.
- Chiffrement autosynchronisant, analyse spectrale des propriétés de synchronisation.
- Algorithmes sur les courbes elliptiques, multiplication, accouplement, comptage des points.

Carte à puce

Une carte à puce est un rectangle en plastique d'une épaisseur d'1 mm qui porte un circuit intégré (dite puce) capable de mémoriser de façon sécurisée une série d'informations. Elle rassemble un microprocesseur (8 bits et 4 MHz), une mémoire morte ou ROM, une mémoire de stockage et une mémoire vive d'une taille variable selon la somme et la complexité des informations qu'elle va contenir dont leurs protection seront assurer grâce à un code confidentiel dit PIN (Personal Identification Number).

La carte à puce, mono ou multi-applicative, sert d'instrument d'identification personnelle. Badge d'entrée, carte vitale, ou carte SIM, elle acte une identité ou une appartenance. Utilisée sur des cartes bancaires, elle est preuve ou source de paiement. Sa lecture par des équipements spécialisés est réalisée avec ou sans contact avec la puce.

International Workshop on Cryptography and its Applications IWCA' 2016

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

SOUS LE HAUT PATRONAGE DE MONSIEUR LE MINISTRE DE L'ENSEIGNEMENT SUPÉRIEUR ET DE LA RECHERCHE SCIENTIFIQUE

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

26-27 April 2016,

U.S.T.O-MB,

ORAN. ALGERIA

IWCA'16

International Workshop on Cryptography and its Applications

International Workshop sur la Cryptographie et sur ses Applications

Organisée par l'USTO-MB

http://www.univ-usto.dz/ICCA1

ic2016ca@gmail.com

0021341560329 |00213664811717

SCAN ME