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

International Workshop on Cryptography and its Applications - IWCA'16 -

26 & 27 Avril 2016, U.S.T.O-MB, ORAN-ALGERIE

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

Tél : 00213 664811717

☙ 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. Ould Mammar

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	Ouerdia Megherbi, Sarah Kassim, Hamid Hamiche, Saïd Djennoune (***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 Novel Algorithm for Image Encryption Based on Matrix Transformation
14:40-15:00	Sarah Kassim, Hamid Hamiche, Saıd Djennoune, Ouerdia Megherbi, (***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	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. Elhadi Rahmani, M.A. Boudia, (**Univ. Saida**)	Genetic Algorithms Based model for Amelioration of TSZ Cryptosystem

16:20-16:40	Azzouzi Oussama, 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	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 27st

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	Sedat Akleylek, (**Univ. Ondokuz Mayis, 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	Samia Bentaieb and Abdelaziz Ouamri,**(USTO**)	3D Partial Face Recognition using Local Descriptors
11:15-11:35	Ghazli Abdelkader, N. Hadj-Said, A. Ali-Pacha, (**USTO**)	Strong Genetic Stream Cipher Design to Secure Mobile Phone Telepony
11:35-11:55	Assia Beloucif, Lemnouar Noui, (**Univ. Batna**)	Une nouvelle stratégie de chiffrement d'images
12:00-12:50	Oussama Noui and Lemnouar Noui, (**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 andrecommendation**

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

Poster Session 1

Tuesday, April 26th

12:15-12:45	Hentabli Wahiba, 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)
	Nouara Mokhtari, (**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 Bachir Yagoubi,(**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
	K. Ait Saadi, B. Yahya-Zoubir, (**CDTA-Alger)**	Motion detection based motion saliency detection
	S. Selmane, A. ZIDANI, **(Univ. Batna)**	Situated Work Analysis of Attribute-Based Encryption (ABE): Case of Healthcare
	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?
	Nouara Zoubir 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 27st

10:20-10:50	Ghalem kamel ghanem & Hendel fatiha, (**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
	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