**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 Noui, 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, Algeria* | ***A Presentation of a Linear Code over:******”*** |
| **Nacer Ghadbane,** *University M’sila, Algeria* | ***On public key cryptosystem based on the word problem in a group*** |
| **Bilal SAOUD,** *University of Bouira, Algeria* | ***Community structure in complex networks based on Tabu Search”***, |
| **Ahlem Melakhessou,** *University Batna2, Algeria* | ***“*** ***Double Skew (1+u) – Constacyclic codes over***  ***”***, |
| **Karima Djebaili,** *University of Ouragla, Algeria* | ***“A Different Encryption System Based on the Integer Factorization Problem”***, |
| Reguia Lamia Bouzara, *USTHB, Alger, Algeria* | ***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”***, |
| **Ibtissem TALBI,** *Frères Mentouri Constantine University, ALGERIA* | ***“The Skew Tent Map (FSTM) Applied in a New Chaotic Cryptosystem”***, |