*Ministère de l'Enseignement Supérieur et de la Recherche scientifique*

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

*Faculté de Génie Electrique*

*Département d’Electronique*

***La****boratoire de* ***Co****dage et de la* ***S****écurité de l’****I****nformation :* ***LACOSI***

*Second International Workshop on Cryptography and its Applications :* ***2’IWCA’19***

*Organisée par l’USTO-MB*

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



**25 May 2019**

**LIST OF ACCEPTED PAPERS OF *2’IWCA’19***

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **N°** | **Presentation form** | **Authors** | **Title of communication** | **Affiliation** |
| 1 | Poster | Oualid Benamara | Introduction to STARKs: Scalable, transparent, and post-quantum secure computational integrity | *USTHB, Institute of Mathematics, Algeiers* |
| 2 | Oral | Ghalem kamel ghanem | Recognition of individuals from iris images using fusion methods and support vector Machine | Université des Sciences et de la Technologie d’Oran Mohamed Boudiaf, USTO |
| Hendel Fatiha |
| 3 | Poster | Chahira Rouifed | modeling and non linear dynamic analysis of the chaotic Colpitts oscillator up to 1 GHz | Mouloud mammeri university of tizi ouzou |
| Achour Ouslimani | Ecole nationale supérieure de l’électronique et ses applications, Cergy, France |
| Mourad Laghrouche | Mouloud mammeri university of tizi ouzou |
| 4 | Poster | Hana ALI-PACHA | Proposition of a New Vernam Chaotic Cipher | University of Science and Technology of Oran |
| Naima HADJ-SAID |
| Adda ALI-PACHA |
| 5 | Oral |  Mohamed Issad | Efficient FPGA Implementation of ModularMultiplication and Exponentiation | Centre de Développement des Technologies Avancées-CDTA |
| Mohamed Anane | Ecole Supérieure d'Informatique-ESI |
|

|  |  |
| --- | --- |
| Bachir Boudraa |  |

 | USTHB Houari Boumediene, Bab Ezzouar, Alger |
| Ahmed Mohamed

|  |  |
| --- | --- |
| Bellemou |  |

 | Centre de Développement des Technologies Avancées-CDTA |
|

|  |  |
| --- | --- |
| Nadjia Anane |  |

 |
| 6 | Poster | Karima Chatouh | A Presentation of a Linear Code over : | *Mostefa Ben Boulaid* University, Batna 2. Batna |
| 7 | Oral | Lamiche Chaabane | An Improved Encryption Approach Based on Multi-chaotic Maps Applied to Digital Image | Mohamed Boudiaf university M’sila |
| 8 | Oral |  Mohamed Issad | Secure Hybrid Crypto-system AES/RSA on FPGA for Data Communication | Centre de Développement des Technologies Avancées-CDTA |
| Nadjia Anane |
|

|  |  |
| --- | --- |
| Ahmed Mohamed Bellemou |  |

 |
|

|  |  |
| --- | --- |
| Bachir Boudraa |  |

 | USTHB Houari Boumediene, Bab Ezzouar, Alger |
| 9 | Poster | Nacer Ghadbane | On public key cryptosystem based on the word problem in a group | Mohamed Boudiaf university M’sila |
| 10 | Oral | Hichem BOUCHAKOUR ERRAHMANI | A New Approach to Verifying and Sharing a Secret QR Code using Elliptic Curves | Djillali Liabes University Sidi Bel Abbes |
| Hind IKNI | Belhadj Bouchaib Center-University Ain Temouchent, |
| 11 | Oral | *Abdelkader GHAZLI* | Security Enhancements of A5/1 Based Particle Swarm Optimization for Mobile Telecommunication Networks | Tahri Mohamed University of Bechar |
| *Adda ALI-PACHA* | Université des Sciences et de la Technologie d’Oran Mohamed Boudiaf, USTO |
| *Naima HADJ SAID* |
| *Boubakeur Ghazli* | Tahri Mohamed University of Bechar |
| 12 | Oral | DJAMEL BELLAOUAR | Nonstandard notes on the ratio of two expressions formed by the product and the sum of certain multiplicative arithmetic functions | University of Guelma |
| 13 | Oral | Ali HADOUDA | A New Efficient Approach Based on Chaotic Map for Image Encryption | Faculty of Exact and Applied Sciences, Université Oran1 |
| Najia TRACHE |
| Mohamed Fayçal KHELFI |
| 14 | Oral | Mustapha MEFTAH | DNA Encryption Algorithm Based on Variable Coding Scheme | Université des Sciences et de la Technologie d’Oran Mohamed Boudiaf, USTO |
| Adda ALI PACHA |
| Naïma HADJ-SAID |
| 15 | Oral | Rachid RIMANI | Image encryption by AES algorithm based on chaos-Permutation | University Mustapha Stambouli of MASCARA |
| Adda ALI PACHA | Université des Sciences et de la Technologie d’Oran Mohamed Boudiaf, USTO |
| Naïma HADJ-SAID |
| Juan Antonio López RAMOS | University of Almeria SPAIN |
| 16 | Poster | Abdelkader Bouguessa | New Technique of styganography Based on the Theory of Chaos : Survey | Université des Sciences et de la Technologie d’Oran Mohamed Boudiaf, USTO |
| Naïma HADJ-SAID |
| Adda ALI PACHA |
| 17 | Oral | Ahmed Yassine Boumedine | Face Identification using Kinect Depth-Maps under One Sample per Person Scenario | Université des Sciences et de la Technologie d’Oran Mohamed Boudiaf, USTO |
| Samia Bentaieb |
| Abdelaziz Ouamri |
| 18 | Oral | Oussama Noui | A novel image encryption approach using polar decomposition and orthogonal matrices | *University of Batna 1, Algeria* |
| Amine Barkat | *Electronics, Information, and Bioengineering, Politecnico di Milano, Italy* |
| Assia Beloucif | *University of Batna 2, Algeria* |
| 19 | Poster | Bilal SAOUD | Community structure in complex networks based on Tabu Search | *Bouira University,* Bouira |
| 20 | Poster | Noureddine Chikouche | SIMULATION OF ATTACKS ON AUTHENTICATION PROTOCOLS FOR NEAR FIELD COMMUNICATIONS | Mohamed Boudiaf University of M’sila |
| 21 | Oral | Noureddine Chikouche | Privacy Analysis of a New Authentication Protocol for Internet of Things |
| 22 | Poster | Asmaa Aouat | Approach Management Application in Cloud Computing: Runtime vs Docker | *University of Oran1 Ahmed Ben Bella* |
| El Abbassia Deba |
| Abou El Hassan Benyamina |
| 23 | Oral | Mohammed Amine BOUDOUAIA | Approach Management Application in Cloud Computing: Runtime vs Docker | University of Science and Technology of Oran |
| Adda ALI PACHA |
| Pascal LORENZ | University of Haute Alsace, France |
| 24 | Poster | Ahlem Melakhessou | Double Skew (1 + u)-Constacyclic Codes over Z4(Z4 + uZ4) | *Mostefa Ben Boulaıd University* Batna2, Algeria |
| Kenza Guenda | *University of Science and Technology Houari Boumedien* Algiers |
| 25 | Oral | Khaled Hamouid | Anonymous communication in IoT based onverifiable encryption | *Mostefa Ben Boulaıd University* Batna2, Algeria |
| 26 | Oral | Ahmed Sabri | Chaotic Encryption for Fingerprint images | University of Science and Technology of Oran |
| Mohamed Ouslim |
| 27 | Oral | Murat Demircioglu | Efficient GeMSS Based Ring Signature Scheme | *Middle East Technical University* Ankara, Turkey |
| Sedat Akleylek | *Ondokuz Mayis University* Samsun, Turkey |
| Murat Cenk | *Middle East Technical University* Ankara, Turkey |
| 28 | Poster | Karima Djebaili | A Different Encryption System Based on the Integer Factorization Problem | University of Ouargla, |
| Lamine Melkemi | University of Batna 2, Batna |
| 29 | Poster | Reguia Lamia Bouzara | Lifted Codes over Finite Chain Rings | *University of Science and Technology Houari Boumedien* Algiers |
| Edgar Martinez-Moro | *University of Valladolid,* Valladolid, Spain |
| Kenza Guenda | *University of Science and Technology Houari Boumedien* Algiers |
| 30 | Oral | Sihem Mesnager | Three-Weight Minimal Linear Codes and Their Applications | *Universities of Paris VIII and XIII CNRS, UMR 7539 LAGA and Telecom ParisTech,* Paris, France |
| Ahmet Sınak | *Necmettin Erbakan University,* Turkey |
| Oğuz Yayla | *Hacettepe University*Ankara, Turkey |
| 31 | Oral | Mahdjoubi Roumaissa | New Signature Algorithm Based on Concatenated Rank Codes | *University of Science and Technology Houari Boumedien* Algiers |
| Kenza Guenda |
| 32 | Poster | Rekkal kahina | Encrypting the TCM Encoder with Locally Rotated Constellations in Rayleigh Fading Channel | Tahri Mohammed University-Bechar |
| Rekkal Sarah | university of Oran1 ahmed ben bella |
| Abdesselam Bassou | Tahri Mohammed University-Bechar |
| 33 | Poster | Amine Zellagui | Secure MD4 Hash Function Using Henon Map | University of Science and Technology of Oran |
| Naima HADJ-SAID |
| Adda ALI-PACHA |
| 34 | Poster | ALI CHERIF Khalfallah | Using of Multi Chaotic System for Implementing a Good Cryptosystem | University of Science and Technology of Oran |
| Naima HADJ-SAID |
| Adda ALI-PACHA |
| 35 | Poster | Hadj Ahmed BOUARARA | Detection and Prevention of Suicidal Self-harm Behavior in Twitter | *Molay Tahar university of saida algeria* |
| 36 | Poster | BAIDAR Lotfi | PSO Variants for Localization Challenge in Wireless Sensor Network and Internet Of Thing | Ecole Superieure en Informatique, Sidi Bel Abbes, Algeria |
| RAHMOUN Abdellatif |
| LORENZ Pascal | IUT of Colmar, University of Haute Alsace, Mulhouse *,*France |
| Miloud Mihoubi | Djillali Liabes University, Sidi Bel Abbes, Algeria |
| 37 | Oral | LAAJI EL Hassane | Two new Quantum Attack Algorithms against NTRU pke # KA NTRU # & # PA NTRU #. | Mohammed First University, Oujda, Morocco |
| AZIZI Abdelmalek |
| AZZOUAK Siham | Sidi Mahammed Ben Abdellah University, Fes, Morocco |
| 38 | Poster | Hebbache Zineb | Study On Skew Codes over The ring Zq + uZq | Univesity of Science and Technology Houari Boumedien, Algiers, Algeria |
| Guenda Kenza |
| 39 | Oral | SAOUDI Mohamed | Efficient Hardware Implementation of Elliptic Curve Diffie-Hellman Key Exchange Protocol | ***Department of Electronics, ESACH/Algiers, Algeria*** |
| KERMICH Akram |
| ZEBDA abdelfatah |
| ALLAILOU Boufeldja |
| 40 | Poster |  Salah Salim Belaifa | Authentication, Cyphering & Security in Modern Mobile Network | Technology/ T.NOC. Transmission, Djezzy Telecom Algeria |
| 41 | Oral | BENHADDAD Omar Hocine | Hardware Acceleration of AES Cryptographic Algorithm for IPsec | ***Department of Electronics, ESACH/Algiers, Algeria*** |
| SAOUDI Mohamed |
| DROUICHE Amine |
| RABIAI Mohamed |
| ALLAILOU Boufeldja |
| 42 | Poster | Farah Bahmed | Hand Biometry: A Review | *Ahmed Zabana University Centre, Relizane, Algeria* |
| Madani Ould Mammar | *University Abdelhamid Ibn Badis, Mostaganem, Algeria* |
| 43 | Oral | Moussaoui Sarah | Implementation and statistical tests of a blockcipher algorithm MISTY1 | ***Laboratoire Centrale de R&D, ECRMT/Algiers, Algeria*** |
| Zeghdoud Sabrina |
| Allailou Boufeldja |
| 44 | Poster | Ibtissem TALBI | The Skew Tent Map (FSTM) Applied in a New Chaotic Cryptosystem | *Frères Mentouri Constantine University, ALGERIA* |
| Soraya BOUGHABA |