C2SI-Berger2015
May 26-28, 2015, Rabat, Morocco

Tuesday, May 26, 2015

08:00 – 09:00 **Registration**

09:00 – 09:45 **Invited talk 1:** **Chair: Thierry Berger**
Differential attacks against SPN: a thorough analysis
Anne Canteaut (with Joëlle Roué)

Session 1: **Codes I** **Chair: Claude Carlet**

1) 09:45 – 10:15 **CUBE Cipher: A Family of Quasi-Involutive Block Ciphers Easy to Mask**
Thierry P. Berger, Julien Francq and Marine Minier

2) 10:15 – 10:45 **Repeated-Root Isodual Cyclic Codes over Finite Fields**
Aicha Batoul, Kenza Guenda and T. Aaron Gulliver

10:45 – 11:15 **Coffee break**

Session 2: **Cryptanalysis I** **Chair: François Arnault**

3) 11:15 – 11:45 **Factoring RSA moduli with weak prime factors**
Abderrahmane Nitaj and Tajjeeddine Rachidi

4) 11:45 – 12:15 **New attacks on RSA with Moduli $N=p^rq$**
Abderrahmane Nitaj and Tajjeeddine Rachidi

12:15 – 14:00 **Lunch break**

14:00 – 14:45 **Invited talk 2:** **Chair: El Mamoun Souidi**
On the properties of vectorial functions with plateaued components and their consequences on APN
Claude Carlet

Session 3: **Cryptanalysis II** **Chair: Abderrahmane Nitaj**

5) 14:45 – 15:15 **A Higher Order Key Partitioning Attack with Application to LBlock**
Riham AlTawy, Mohamed Tolba, and Amr M. Youssef

6) 15:15 – 15:45 **Countermeasures Mitigation for Designing Rich Shell Code in Java Card**
Noreddine El Janati El Idrissi, Said El Hajji and Jean-Louis Lanet

7) 15:45 – 16:15 **Square Code Attack on a Modified Sidelnikov Cryptosystem**
Ayoub Otmani and Hervé Talé Kalachi

16:15 – 16:45 **Coffee break**

16:45 – 17:45 **Conference official ceremony**

Wednesday, May 27, 2015

09:00 – 09:45	**Invited talk 3:**	**Chair: Anne Canteaut**
	On the Security of Long-lived Archiving Systems based on the Evidence Record Syntax Johannes Buchmann (with Matthias Geihs, Denise Demirel)	
Session 4:	**Protocols**	**Chair: Anne Canteaut**
8) 09:45 – 10:15	**Weaknesses in Two RFID Authentication Protocols** Noureddine Chikouche, Foudil Cherif, Pierre-Louis Cayrel, and Mohamed Benmohammed	
9) 10:15 – 10:45	**A Dynamic Attribute-based Authentication Scheme** Huihui Yang, Vladimir A Oleshchuk	
10:45 – 11:15	**Coffee break**	
11:15 – 12:00	**Invited talk 4:**	**Chair: Tajjeeddine Rachidi**
	Multidimensional Bell inequalities and quantum cryptography François Arnault	
12:00 – 14:00	**Lunch break**	
Session 5:	**Codes II**	**Chair: Johannes Buchmann**
10) 14:00 – 14:30	**A Family of Six-Weight Reducible Cyclic Codes and their Weight Distribution** Gerardo Vega	
11) 14:30 – 15:00	**Codes over L(GF(2)^m,GF(2)^m), MDS diffusion matrices and cryptographic applications** Thierry P. Berger and Nora El Amrani	
15:00 – 15:45	**Invited talk 5:**	**Chair: Marine Minier**
	Securing the Web of Things With Role-Based Access Control Ezedin Barka (with Sujith Samuel Mathew, and Yacine Atif)	
15:45 – 16:15	**Coffee break**	
Session 6:	**Security**	**Chair: Jean-Louis Lanet**
12) 16:15 – 16:45	**Formal enforcement of security policies on parallel systems with risk integration** Marwa Ziadia and Mohamed Mejri	
13) 16:45 – 17:15	**Algorithms of Constructing Linear and Robust Codes Based on Wavelet Decomposition and its Application** Alla Levina and Sergey Taranov	
14) 17:15 – 17:45	**Security Issues on Inter-Domain Routing with QoS-CMS Mechanism** Hafssa Benaboud, Sara Bakkali and José Johnny Randriamampionona	
15) 17:45 – 18:15	**Impossible Differential Properties of Reduced Round Streebog** Ahmed Abdelkhalek, Riham AlTawy, and Amr M. Youssef	

Thursday, May 28, 2015

09:00 – 09:45	**Invited talk 6:**	**Chair: El Mamoun Souidi**
	Beyond Cryptanalysis is Software Security the Next Threat for Smart Cards Jean-Louis Lanet	
Session 7:	**Codes III**	**Chair: Felix Ulmer**
16) 09:45 – 10:15	**A note on the existence of self-dual skew codes over finite fields** Delphine Boucher	
17) 10:15 – 10:45	**The Weight Distribution of a Family of Lagrangian-Grassmannian Codes** Jesus Carrillo-Pacheco and Gerardo Vega	
10:45 – 11:15	**Coffee break**	
Session 8:	**Elliptic Curves**	**Chair: Abderrahmane Nitaj**
18) 11:15 – 11:45	**Failure of the Point Blinding Countermeasure against Fault Attack in Pairing-Based Cryptography** Nadia El Mrabet and Emmanuel Fouotsa	
12:00 – 14:00	**Lunch break**	
14:00 – 14:45	**Invited talk 7:**	**Chair: Claude Carlet**
	Codes as modules over skew polynomial rings Felix Ulmer	
Session 9:	**Algorithms**	**Chair: Ezedin Barka**
19) 14:45 – 15:15	**Performance of LDPC Decoding Algorithms with a Statistical Physics Theory Approach** Manel Abdelhedi, Omessaad Hamdi and Ammar Bouallegue	
15:15 – 15:45	**Coffee break**	
20) 15:45 – 16:15	**Representation of Dorsal Hand Vein Pattern Using Local Binary Patterns (LBP)** Maleika Heenaye Mamode Khan	
21) 16:15 – 16:45	**Watermarking based Multi-Biometric Fusion Approach** Sanaa Ghouzali	
16:45 – 17:00	**Closing remarks**	