

# Contents

## Invited Papers

Multidimensional Bell Inequalities and Quantum Cryptography .....	3
<i>François Arnault</i>	
Securing the Web of Things with Role-Based Access Control .....	14
<i>Ezedine Barka, Sujith Samuel Mathew, and Yacine Atif</i>	
On the Security of Long-Lived Archiving Systems Based on the Evidence Record Syntax .....	27
<i>Matthias Geihs, Denise Demirel, and Johannes Buchmann</i>	
Differential Attacks Against SPN: A Thorough Analysis .....	45
<i>Anne Canteaut and Joëlle Roué</i>	
On the Properties of Vectorial Functions with Plateaued Components and Their Consequences on APN Functions .....	63
<i>Claude Carlet</i>	
Beyond Cryptanalysis Is Software Security the Next Threat for Smart Cards .....	74
<i>Jean-Louis Lanet</i>	
Extended Abstract: Codes as Modules over Skew Polynomial Rings.....	83
<i>Felix Ulmer</i>	

## Regular Papers

CUBE Cipher: A Family of Quasi-Involutive Block Ciphers Easy to Mask.....	89
<i>Thierry P. Berger, Julien Francq, and Marine Minier</i>	
A Dynamic Attribute-Based Authentication Scheme .....	106
<i>Huihui Yang and Vladimir A. Oleshchuk</i>	
Repeated-Root Isodual Cyclic Codes over Finite Fields .....	119
<i>Aicha Batoul, Kenza Guenda, and T. Aaron Gulliver</i>	
Formal Enforcement of Security Policies on Parallel Systems with Risk Integration .....	133
<i>Marwa Ziadia and Mohamed Mejri</i>	
Countermeasures Mitigation for Designing Rich Shell Code in Java Card .....	149
<i>Noredidine El Janati El Idrissi, Said El Hajji, and Jean-Louis Lanet</i>	

Weaknesses in Two RFID Authentication Protocols .....	162
<i>Noureddine Chikouche, Foudil Cherif, Pierre-Louis Cayrel, and Mohamed Benmohammed</i>	
Square Code Attack on a Modified Sidelnikov Cryptosystem .....	173
<i>Ayoub Otmani and Hervé Talé Kalachi</i>	
A Family of Six-Weight Reducible Cyclic Codes and their Weight Distribution .....	184
<i>Gerardo Vega</i>	
Codes over $\mathcal{L}(GF(2)^m, GF(2)^m)$ , MDS Diffusion Matrices and Cryptographic Applications .....	197
<i>Thierry P. Berger and Nora El Amrani</i>	
A Higher Order Key Partitioning Attack with Application to LBlock ...	215
<i>Riham AlTawy, Mohamed Tolba, and Amr M. Youssef</i>	
A Note on the Existence of Self-Dual Skew Codes over Finite Fields ....	228
<i>Delphine Boucher</i>	
The Weight Distribution of a Family of Lagrangian-Grassmannian Codes .....	240
<i>Jesús Carrillo-Pacheco, Gerardo Vega, and Felipe Zaldívar</i>	
Algorithms of Constructing Linear and Robust Codes Based on Wavelet Decomposition and Its Application .....	247
<i>Alla Levina and Sergey Taranov</i>	
Failure of the Point Blinding Countermeasure Against Fault Attack in Pairing-Based Cryptography .....	259
<i>Nadia El Mrabet and Emmanuel Fouotsa</i>	
Impossible Differential Properties of Reduced Round Streebog .....	274
<i>Ahmed Abdelkhalek, Riham AlTawy, and Amr M. Youssef</i>	
Security Issues on Inter-Domain Routing with QoS-CMS Mechanism ...	287
<i>Hafssa Benaboud, Sara Bakkali, and José Johnny Randriamampionona</i>	
Uncovering Self Code Modification in Android .....	297
<i>Faisal Nasim, Baber Aslam, Waseem Ahmed, and Talha Naeem</i>	
Performance of LDPC Decoding Algorithms with a Statistical Physics Theory Approach .....	314
<i>Manel Abdelhedi, Omessaad Hamdi, and Ammar Bouallegue</i>	
Representation of Dorsal Hand Vein Pattern Using Local Binary Patterns (LBP) .....	331
<i>Maleika Heenaye Mamode Khan</i>	

Watermarking Based Multi-biometric Fusion Approach .....	342
<i>Sanaa Ghouzali</i>	
New Attacks on RSA with Moduli $N = p^r q$ .....	352
<i>Abderrahmane Nitaj and Tajjeeddine Rachidi</i>	
Factoring RSA Moduli with Weak Prime Factors.....	361
<i>Abderrahmane Nitaj and Tajjeeddine Rachidi</i>	
<b>Author Index</b> .....	375

Codes, Cryptology, and Information Security  
First International Conference, C2SI 2015, Rabat,  
Morocco, May 26-28, 2015, Proceedings - In Honor of  
Thierry Berger  
El Hajji, S.; Nitaj, A.; Carlet, C.; Souidi, E.M. (Eds.)  
2015, XXVI, 375 p. 58 illus., Softcover  
ISBN: 978-3-319-18680-1