

# Contents

## Invited Papers

Some Results on the Known Classes of Quadratic APN Functions . . . . .	3
<i>Lilya Budaghyan, Tor Helleseth, Nian Li, and Bo Sun</i>	
Families of Convolutional Codes over Finite Fields: A Survey . . . . .	17
<i>M. Isabel García-Planas</i>	
Codes for Side-Channel Attacks and Protections . . . . .	35
<i>Sylvain Guilley, Annelie Heuser, and Olivier Rioul</i>	
An Overview of the State-of-the-Art of Cloud Computing Cyber-Security . . .	56
<i>H. Bennisar, A. Bendahmane, and M. Essaïdi</i>	
Somewhat/Fully Homomorphic Encryption: Implementation Progresses and Challenges . . . . .	68
<i>Guillaume Bonnoron, Caroline Fontaine, Guy Gogniat, Vincent Herbert, Vianney Lapôtre, Vincent Migliore, and Adeline Roux-Langlois</i>	

## Regular Papers

Two-Source Randomness Extractors for Elliptic Curves for Authenticated Key Exchange . . . . .	85
<i>Abdoul Aziz Ciss and Djiby Sow</i>	
Generalization of BJMM-ISD Using May-Ozerov Nearest Neighbor Algorithm over an Arbitrary Finite Field $\mathbb{F}_q$ . . . . .	96
<i>Cheikh Thiécoumba Gueye, Jean Belo Klamti, and Shoichi Hirose</i>	
Parameters of 2-Designs from Some BCH Codes . . . . .	110
<i>Cunsheng Ding and Zhengchun Zhou</i>	
A Median Nearest Neighbors LDA for Anomaly Network Detection . . . . .	128
<i>Zyad Elkhadir, Khalid Chougali, and Mohammed Benattou</i>	
Linearly Homomorphic Authenticated Encryption with Provable Correctness and Public Verifiability . . . . .	142
<i>Patrick Struck, Lucas Schabhüser, Denise Demirel, and Johannes Buchmann</i>	
Constacyclic Codes over Finite Principal Ideal Rings . . . . .	161
<i>Aicha Batoul, Kenza Guenda, T. Aaron Gulliver, and Nuh Aydin</i>	

On Isodual Cyclic Codes over Finite Chain Rings. . . . .	176
<i>Aicha Batoul, Kenza Guenda, T. Aaron Gulliver, and Nuh Aydin</i>	
Revisiting the Efficient Key Generation of ZHFE . . . . .	195
<i>Yasuhiko Ikematsu, Dung H. Duong, Albrecht Petzoldt, and Tsuyoshi Takagi</i>	
The Weight Distribution for an Extended Family of Reducible Cyclic Codes . . . . .	213
<i>Gerardo Vega and Jesús E. Cuén-Ramos</i>	
A NP-Complete Problem in Coding Theory with Application to Code Based Cryptography . . . . .	230
<i>Thierry P. Berger, Cheikh Thiécoumba Gueye, and Jean Belo Klamti</i>	
Spectral Approach for Correlation Power Analysis . . . . .	238
<i>Philippe Guillot, Gilles Millérioux, Brandon Dravie, and Nadia El Mrabet</i>	
Efficient Implementation of Hybrid Encryption from Coding Theory . . . . .	254
<i>Pierre-Louis Cayrel, Cheikh Thiecoumba Gueye, El Hadji Modou Mboup, Ousmane Ndiaye, and Edoardo Persichetti</i>	
On the Multi-output Filtering Model and Its Applications. . . . .	265
<i>Teng Wu, Yin Tan, Kalikinkar Mandal, and Guang Gong</i>	
New Bent Functions from Permutations and Linear Translators. . . . .	282
<i>Siheem Mesnager, Pinar Ongan, and Ferruh Özbudak</i>	
Bent Functions in $\mathcal{C}$ and $\mathcal{D}$ Outside the Completed Maiorana-McFarland Class. . . . .	298
<i>F. Zhang, E. Pasalic, N. Cepak, and Y. Wei</i>	
Quantum Algorithms Related to $HN$ -Transforms of Boolean Functions . . . . .	314
<i>Sugata Gangopadhyay, Subhamoy Maitra, Nishant Sinha, and Pantelimon Stănică</i>	
Explicit Characterizations for Plateaued-ness of $p$ -ary (Vectorial) Functions . . . . .	328
<i>Claude Carlet, Siheem Mesnager, Ferruh Özbudak, and Ahmet Sinak</i>	
A New Dynamic Code-Based Group Signature Scheme . . . . .	346
<i>Berenger Edoukou Ayebe, Hafsa Assidi, and El Mamoun Souidi</i>	
A Secure Cloud-Based IDPS Using Cryptographic Traces and Revocation Protocol . . . . .	365
<i>Hind Idrissi, Mohammed Ennahbaoui, Said El Hajji, and El Mamoun Souidi</i>	
<b>Author Index</b> . . . . .	383

<http://www.springer.com/978-3-319-55588-1>

Codes, Cryptology and Information Security  
Second International Conference, C2SI 2017, Rabat,  
Morocco, April 10–12, 2017, Proceedings - In Honor of  
Claude Carlet

El Hajji, S.; Nitaj, A.; Souidi, E.M. (Eds.)

2017, XII, 384 p. 46 illus., Softcover

ISBN: 978-3-319-55588-1