

Table of Contents

Using LDGM Codes and Sparse Syndromes to Achieve Digital Signatures	1
<i>Marco Baldi, Marco Bianchi, Franco Chiaraluce, Joachim Rosenthal, and Davide Schipani</i>	
Quantum Algorithms for the Subset-Sum Problem	16
<i>Daniel J. Bernstein, Stacey Jeffery, Tanja Lange, and Alexander Meurer</i>	
Improved Lattice-Based Threshold Ring Signature Scheme	34
<i>Slim Bettaieb and Julien Schrek</i>	
Degree of Regularity for HFEv and HFEv-	52
<i>Jintai Ding and Bo-Yin Yang</i>	
Software Speed Records for Lattice-Based Signatures	67
<i>Tim Güneysu, Tobias Oder, Thomas Pöppelmann, and Peter Schwabe</i>	
Solving the Shortest Vector Problem in Lattices Faster Using Quantum Search	83
<i>Thijs Laarhoven, Michele Mosca, and Joop van de Pol</i>	
An Efficient Attack of a McEliece Cryptosystem Variant Based on Convolutional Codes	102
<i>Grégory Landaïs and Jean-Pierre Tillich</i>	
Extended Algorithm for Solving Underdefined Multivariate Quadratic Equations	118
<i>Hiroyuki Miura, Yasufumi Hashimoto, and Tsuyoshi Takagi</i>	
Quantum Key Distribution in the Classical Authenticated Key Exchange Framework	136
<i>Michele Mosca, Douglas Stebila, and Berkant Ustaoglu</i>	
Cryptanalysis of Hash-Based Tamed Transformation and Minus Signature Scheme	155
<i>Xuyun Nie, Zhaohu Xu, and Johannes Buchmann</i>	
A Classification of Differential Invariants for Multivariate Post-quantum Cryptosystems	165
<i>Ray Perlner and Daniel Smith-Tone</i>	

Secure and Anonymous Hybrid Encryption from Coding Theory 174
 Edoardo Persichetti

Fast Verification for Improved Versions of the UOV and Rainbow
Signature Schemes 188
 Albrecht Petzoldt, Stanislav Bulygin, and Johannes Buchmann

The Hardness of Code Equivalence over $\mathbb{F}_q$ and Its Application to
Code-Based Cryptography 203
 Nicolas Sendrier and Dimitris E. Simos

Timing Attacks against the Syndrome Inversion in Code-Based
Cryptosystems 217
 Falko Strenzke

Simple Matrix Scheme for Encryption 231
 Chengdong Tao, Adama Diene, Shaohua Tang, and Jintai Ding

Multivariate Signature Scheme Using Quadratic Forms 243
 Takanori Yasuda, Tsuyoshi Takagi, and Kouichi Sakurai

Author Index 259