

# Contents

## Code-Based Cryptography

A New Rank Metric Codes Based Encryption Scheme. . . . .	3
<i>Pierre Loidreau</i>	
Ouroboros: A Simple, Secure and Efficient Key Exchange Protocol Based on Coding Theory . . . . .	18
<i>Jean-Christophe Deneuville, Philippe Gaborit, and Gilles Zémor</i>	
CCA2 Key-Privacy for Code-Based Encryption in the Standard Model . . . . .	35
<i>Yusuke Yoshida, Kirill Morozov, and Keisuke Tanaka</i>	
A Reaction Attack on the QC-LDPC McEliece Cryptosystem. . . . .	51
<i>Tomáš Fabšič, Viliam Hromada, Paul Stankovski, Pavol Zajac, Qian Guo, and Thomas Johansson</i>	
Quantum Information Set Decoding Algorithms . . . . .	69
<i>Ghazal Kachigar and Jean-Pierre Tillich</i>	

## Isogeny-Based Cryptography

Loop-Abort Faults on Supersingular Isogeny Cryptosystems. . . . .	93
<i>Alexandre Gélín and Benjamin Wesolowski</i>	
Fault Attack on Supersingular Isogeny Cryptosystems . . . . .	107
<i>Yan Bo Ti</i>	

## Lattice-Based Cryptography

Fast Lattice-Based Encryption: Stretching SPRING . . . . .	125
<i>Charles Bouillaguet, Claire Delaplace, Pierre-Alain Fouque, and Paul Kirchner</i>	
Revisiting TESLA in the Quantum Random Oracle Model. . . . .	143
<i>Erdem Alkim, Nina Bindel, Johannes Buchmann, Özgür Dagdelen, Edward Eaton, Gus Gutoski, Juliane Krämer, and Filip Pawlega</i>	
Cryptanalysis of RLWE-Based One-Pass Authenticated Key Exchange . . . . .	163
<i>Boru Gong and Yunlei Zhao</i>	
A Hybrid Lattice Basis Reduction and Quantum Search Attack on LWE . . . . .	184
<i>Florian Göpfert, Christine van Vredendaal, and Thomas Wunderer</i>	

**Multivariate Cryptography**

HMFE<sub>v</sub> - An Efficient Multivariate Signature Scheme . . . . . 205  
*Albrecht Petzoldt, Ming-Shing Chen, Jintai Ding, and Bo-Yin Yang*

MQ Signatures for PKI . . . . . 224  
*Alan Szepieniec, Ward Beullens, and Bart Preneel*

An Updated Security Analysis of PFLASH . . . . . 241  
*Ryann Cartor and Daniel Smith-Tone*

Improved Attacks for Characteristic-2 Parameters of the Cubic ABC  
Simple Matrix Encryption Scheme . . . . . 255  
*Dustin Moody, Ray Perlner, and Daniel Smith-Tone*

Key Recovery Attack for All Parameters of HFE- . . . . . 272  
*Jeremy Vates and Daniel Smith-Tone*

Key Recovery Attack for ZHFE . . . . . 289  
*Daniel Cabarcas, Daniel Smith-Tone, and Javier A. Verbel*

**Quantum Algorithms**

Post-quantum RSA . . . . . 311  
*Daniel J. Bernstein, Nadia Heninger, Paul Lou, and Luke Valenta*

A Low-Resource Quantum Factoring Algorithm . . . . . 330  
*Daniel J. Bernstein, Jean-François Biasse, and Michele Mosca*

Quantum Algorithms for Computing Short Discrete Logarithms  
and Factoring RSA Integers . . . . . 347  
*Martin Ekerå and Johan Håstad*

**Security Models**

XOR of PRPs in a Quantum World. . . . . 367  
*Bart Mennink and Alan Szepieniec*

Transitioning to a Quantum-Resistant Public Key Infrastructure . . . . . 384  
*Nina Bindel, Udyani Herath, Matthew McKague, and Douglas Stebila*

ORAMs in a Quantum World. . . . . 406  
*Tommaso Gagliardoni, Nikolaos P. Karvelas, and Stefan Katzenbeisser*

**Author Index** . . . . . 427



<http://www.springer.com/978-3-319-59878-9>

Post-Quantum Cryptography

8th International Workshop, PQCrypto 2017, Utrecht,

The Netherlands, June 26-28, 2017, Proceedings

Lange, T.; Takagi, T. (Eds.)

2017, XII, 427 p. 34 illus., Softcover

ISBN: 978-3-319-59878-9