

# Contents

IND-CCA Secure Hybrid Encryption from QC-MDPC Niederreiter . . . . .	1
<i>Ingo von Maurich, Lukas Heberle, and Tim Güneysu</i>	
RankSynd a PRNG Based on Rank Metric. . . . .	18
<i>Philippe Gaborit, Adrien Hauteville, and Jean-Pierre Tillich</i>	
Applying Grover’s Algorithm to AES: Quantum Resource Estimates. . . . .	29
<i>Markus Grassl, Brandon Langenberg, Martin Roetteler, and Rainer Steinwandt</i>	
Post-Quantum Security of the CBC, CFB, OFB, CTR, and XTS Modes of Operation. . . . .	44
<i>Mayuresh Vivekanand Anand, Ehsan Ebrahimi Targhi, Gelo Noel Tabia, and Dominique Unruh</i>	
Post-Quantum Security Models for Authenticated Encryption . . . . .	64
<i>Vladimir Soukharev, David Jao, and Srinath Seshadri</i>	
Quantum Collision-Resistance of Non-uniformly Distributed Functions . . . . .	79
<i>Ehsan Ebrahimi Targhi, Gelo Noel Tabia, and Dominique Unruh</i>	
An Efficient Attack on a Code-Based Signature Scheme . . . . .	86
<i>Aurélie Phesso and Jean-Pierre Tillich</i>	
Vulnerabilities of “McEliece in the World of Escher” . . . . .	104
<i>Dustin Moody and Ray Perlner</i>	
Cryptanalysis of the McEliece Public Key Cryptosystem Based on Polar Codes . . . . .	118
<i>Magali Bardet, Julia Chaulet, Vlad Dragoi, Ayoub Otmani, and Jean-Pierre Tillich</i>	
Analysis of Information Set Decoding for a Sub-linear Error Weight. . . . .	144
<i>Rodolfo Canto Torres and Nicolas Sendrier</i>	
On the Differential Security of the HFEv- Signature Primitive . . . . .	162
<i>Ryann Cartor, Ryan Gipson, Daniel Smith-Tone, and Jeremy Vates</i>	
Extension Field Cancellation: A New Central Trapdoor for Multivariate Quadratic Systems. . . . .	182
<i>Alan Szepieniec, Jintai Ding, and Bart Preneel</i>	
Security Analysis and Key Modification for ZHFE . . . . .	197
<i>Ray Perlner and Daniel Smith-Tone</i>	

Efficient ZHFE Key Generation . . . . .	213
<i>John B. Baena, Daniel Cabarcas, Daniel E. Escudero,</i> <i>Jaiberth Porras-Barrera, and Javier A. Verbel</i>	
Additively Homomorphic Ring-LWE Masking . . . . .	233
<i>Oscar Reparaz, Ruan de Clercq, Sujoy Sinha Roy, Frederik Vercauteren,</i> <i>and Ingrid Verbauwhede</i>	
A Homomorphic LWE Based E-voting Scheme . . . . .	245
<i>Ilaria Chillotti, Nicolas Gama, Mariya Georgieva,</i> <i>and Malika Izabachène</i>	
<b>Author Index</b> . . . . .	267

Post-Quantum Cryptography

7th International Workshop, PQCrypto 2016, Fukuoka,  
Japan, February 24-26, 2016, Proceedings

Takagi, T. (Ed.)

2016, X, 267 p. 39 illus. in color., Softcover

ISBN: 978-3-319-29359-2