

## Contents – Part II

### Asiacrypt 2017 Award Paper I

Kummer for Genus One over Prime Order Fields . . . . .	3
<i>Sabyasachi Karati and Palash Sarkar</i>	

### Pairing-based Protocols

ABE with Tag Made Easy: Concise Framework and New Instantiations in Prime-Order Groups . . . . .	35
<i>Jie Chen and Junqing Gong</i>	
Towards a Classification of Non-interactive Computational Assumptions in Cyclic Groups. . . . .	66
<i>Essam Ghadafi and Jens Groth</i>	
An Efficient Pairing-Based Shuffle Argument. . . . .	97
<i>Prastudy Fauzi, Helger Lipmaa, Janno Siim, and Michał Zając</i>	
Efficient Ring Signatures in the Standard Model. . . . .	128
<i>Giulio Malavolta and Dominique Schröder</i>	

### Quantum Algorithms

Grover Meets Simon – Quantumly Attacking the FX-construction. . . . .	161
<i>Gregor Leander and Alexander May</i>	
Quantum Multicollision-Finding Algorithm . . . . .	179
<i>Akinori Hosoyamada, Yu Sasaki, and Keita Xagawa</i>	
An Efficient Quantum Collision Search Algorithm and Implications on Symmetric Cryptography. . . . .	211
<i>André Chailloux, María Naya-Plasencia, and André Schrottenloher</i>	
Quantum Resource Estimates for Computing Elliptic Curve Discrete Logarithms . . . . .	241
<i>Martin Roetteler, Michael Naehrig, Krysta M. Svore, and Kristin Lauter</i>	

### Elliptic Curves

qDSA: Small and Secure Digital Signatures with Curve-Based Diffie–Hellman Key Pairs . . . . .	273
<i>Joost Renes and Benjamin Smith</i>	

A Simple and Compact Algorithm for SIDH with Arbitrary Degree Isogenies. . . . .	303
<i>Craig Costello and Huseyin Hisil</i>	
Faster Algorithms for Isogeny Problems Using Torsion Point Images . . . . .	330
<i>Christophe Petit</i>	
<b>Block Chains</b>	
Beyond Hellman’s Time-Memory Trade-Offs with Applications to Proofs of Space. . . . .	357
<i>Hamza Abusalah, Joël Alwen, Bram Cohen, Danylo Khilko, Krzysztof Pietrzak, and Leonid Reyzin</i>	
The Sleepy Model of Consensus. . . . .	380
<i>Rafael Pass and Elaine Shi</i>	
Instantaneous Decentralized Poker. . . . .	410
<i>Iddo Bentov, Ranjit Kumaresan, and Andrew Miller</i>	
<b>Multi-party Protocols</b>	
More Efficient Universal Circuit Constructions . . . . .	443
<i>Daniel Günther, Ágnes Kiss, and Thomas Schneider</i>	
Efficient Scalable Constant-Round MPC via Garbled Circuits. . . . .	471
<i>Aner Ben-Efraim, Yehuda Lindell, and Eran Omri</i>	
Overlaying Conditional Circuit Clauses for Secure Computation . . . . .	499
<i>W. Sean Kennedy, Vladimir Kolesnikov, and Gordon Wilfong</i>	
JIMU: Faster LEGO-Based Secure Computation Using Additive Homomorphic Hashes . . . . .	529
<i>Ruiyu Zhu and Yan Huang</i>	
<b>Operating Modes Security Proofs</b>	
Analyzing Multi-key Security Degradation . . . . .	575
<i>Atul Luykx, Bart Mennink, and Kenneth G. Paterson</i>	
Full-State Keyed Duplex with Built-In Multi-user Support . . . . .	606
<i>Joan Daemen, Bart Mennink, and Gilles Van Assche</i>	
Improved Security for OCB3 . . . . .	638
<i>Ritam Bhaumik and Mridul Nandi</i>	

The Iterated Random Function Problem . . . . .	667
<i>Ritam Bhaumik, Nilanjan Datta, Avijit Dutta, Nicky Mouha,</i>	
<i>and Mridul Nandi</i>	
<b>Author Index</b> . . . . .	699

Advances in Cryptology – ASIACRYPT 2017  
23rd International Conference on the Theory and  
Applications of Cryptology and Information Security,  
Hong Kong, China, December 3–7, 2017, Proceedings,  
Part II

Takagi, T.; Peyrin, Th. (Eds.)

2017, XIX, 701 p. 98 illus., Softcover

ISBN: 978-3-319-70696-2