

Contents – Part I

Asiacrypt 2017 Best Paper

Identification Protocols and Signature Schemes Based on Supersingular Isogeny Problems	3
<i>Steven D. Galbraith, Christophe Petit, and Javier Silva</i>	

Post-Quantum Cryptography

An Existential Unforgeable Signature Scheme Based on Multivariate Quadratic Equations	37
<i>Kyung-Ah Shim, Cheol-Min Park, and Namhun Koo</i>	
Post-quantum Security of Fiat-Shamir	65
<i>Dominique Unruh</i>	

Symmetric Key Cryptanalysis

Improved Conditional Cube Attacks on Keccak Keyed Modes with MILP Method	99
<i>Zheng Li, Wenquan Bi, Xiaoyang Dong, and Xiaoyun Wang</i>	
Automatic Search of Bit-Based Division Property for ARX Ciphers and Word-Based Division Property	128
<i>Ling Sun, Wei Wang, and Meiqin Wang</i>	
Collisions and Semi-Free-Start Collisions for Round-Reduced RIPEMD-160	158
<i>Fukang Liu, Florian Mendel, and Gaoli Wang</i>	
Linear Cryptanalysis of DES with Asymmetries	187
<i>Andrey Bogdanov and Philip S. Vejre</i>	
Yoyo Tricks with AES	217
<i>Sondre Rønjom, Navid Ghaedi Bardeh, and Tor Helleseth</i>	
New Key Recovery Attacks on Minimal Two-Round Even-Mansour Ciphers.	244
<i>Takanori Isobe and Kyoji Shibutani</i>	

Lattices

Large Modulus Ring-LWE \geq Module-LWE	267
<i>Martin R. Albrecht and Amit Deo</i>	
Revisiting the Expected Cost of Solving uSVP and Applications to LWE . . .	297
<i>Martin R. Albrecht, Florian Göpfert, Fernando Virdia, and Thomas Wunderer</i>	
Coded-BKW with Sieving	323
<i>Qian Guo, Thomas Johansson, Erik Mårtensson, and Paul Stankovski</i>	
Sharper Bounds in Lattice-Based Cryptography Using the Rényi Divergence	347
<i>Thomas Prest</i>	

Homomorphic Encryptions

Faster Packed Homomorphic Operations and Efficient Circuit Bootstrapping for TFHE	377
<i>Ilaria Chillotti, Nicolas Gama, Mariya Georgieva, and Malika Izabachène</i>	
Homomorphic Encryption for Arithmetic of Approximate Numbers	409
<i>Jung Hee Cheon, Andrey Kim, Miran Kim, and Yongsoo Song</i>	
Quantum Fully Homomorphic Encryption with Verification	438
<i>Gorjan Alagic, Yfke Dulek, Christian Schaffner, and Florian Speelman</i>	

Access Control

Access Control Encryption for General Policies from Standard Assumptions	471
<i>Sam Kim and David J. Wu</i>	
Strengthening Access Control Encryption	502
<i>Christian Badertscher, Christian Matt, and Ueli Maurer</i>	
Adaptive Oblivious Transfer with Access Control from Lattice Assumptions	533
<i>Benoît Libert, San Ling, Fabrice Mouhartem, Khoa Nguyen, and Huaxiong Wang</i>	

Oblivious Protocols

On the Depth of Oblivious Parallel RAM	567
<i>T.-H. Hubert Chan, Kai-Min Chung, and Elaine Shi</i>	

Low Cost Constant Round MPC Combining BMR and Oblivious Transfer	598
<i>Carmit Hazay, Peter Scholl, and Eduardo Soria-Vazquez</i>	
Maliciously Secure Oblivious Linear Function Evaluation with Constant Overhead	629
<i>Satrajit Ghosh, Jesper Buus Nielsen, and Tobias Nilges</i>	
Oblivious Hashing Revisited, and Applications to Asymptotically Efficient ORAM and OPRAM.	660
<i>T.-H. Hubert Chan, Yue Guo, Wei-Kai Lin, and Elaine Shi</i>	
Side Channel Analysis	
Authenticated Encryption in the Face of Protocol and Side Channel Leakage	693
<i>Guy Barwell, Daniel P. Martin, Elisabeth Oswald, and Martijn Stam</i>	
Consolidating Inner Product Masking	724
<i>Josep Balasch, Sebastian Faust, Benedikt Gierlichs, Clara Paglialonga, and François-Xavier Standaert</i>	
The First Thorough Side-Channel Hardware Trojan.	755
<i>Maik Ender, Samaneh Ghandali, Amir Moradi, and Christof Paar</i>	
Amortizing Randomness Complexity in Private Circuits.	781
<i>Sebastian Faust, Clara Paglialonga, and Tobias Schneider</i>	
Author Index	811

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>	

Block Chains

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>	

Multi-party Protocols

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>	

Operating Modes Security Proofs

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
 Ritam Bhaumik, Nilanjan Datta, Avijit Dutta, Nicky Mouha,
 and Mridul Nandi

Author Index 699

Contents – Part III

Asiacrypt 2017 Award Paper II

A Subversion-Resistant SNARK	3
<i>Behzad Abdolmaleki, Karim Bagheri, Helger Lipmaa, and Michał Zając</i>	

Cryptographic Protocols

Two-Round PAKE from Approximate SPH and Instantiations from Lattices	37
<i>Jiang Zhang and Yu Yu</i>	
Tightly-Secure Signatures from Five-Move Identification Protocols	68
<i>Eike Kiltz, Julian Loss, and Jiaxin Pan</i>	
On the Untapped Potential of Encoding Predicates by Arithmetic Circuits and Their Applications.	95
<i>Shuichi Katsumata</i>	
The Minimum Number of Cards in Practical Card-Based Protocols	126
<i>Julia Kastner, Alexander Koch, Stefan Walzer, Daiki Miyahara, Yu-ichi Hayashi, Takaaki Mizuki, and Hideaki Sone</i>	

Foundations

Succinct Spooky Free Compilers Are Not Black Box Sound	159
<i>Zvika Brakerski, Yael Tauman Kalai, and Renen Perlman</i>	
Non-Interactive Multiparty Computation Without Correlated Randomness . . .	181
<i>Shai Halevi, Yuval Ishai, Abhishek Jain, Ilan Komargodski, Amit Sahai, and Eylon Yogev</i>	
Optimal-Rate Non-Committing Encryption	212
<i>Ran Canetti, Oxana Poburinnaya, and Mariana Raykova</i>	
Preventing CLT Attacks on Obfuscation with Linear Overhead.	242
<i>Rex Fernando, Peter M. R. Rasmussen, and Amit Sahai</i>	

Zero-Knowledge Proofs

Two-Message Witness Indistinguishability and Secure Computation in the Plain Model from New Assumptions	275
<i>Saikrishna Badrinarayanan, Sanjam Garg, Yuval Ishai, Amit Sahai, and Akshay Wadia</i>	

Zero-Knowledge Arguments for Lattice-Based PRFs and Applications to E-Cash.	304
<i>Benoît Libert, San Ling, Khoa Nguyen, and Huaxiong Wang</i>	
Linear-Time Zero-Knowledge Proofs for Arithmetic Circuit Satisfiability	336
<i>Jonathan Bootle, Andrea Cerulli, Essam Ghadafi, Jens Groth, Mohammad Hajiabadi, and Sune K. Jakobsen</i>	
Symmetric Key Designs	
How to Use Metaheuristics for Design of Symmetric-Key Primitives.	369
<i>Ivica Nikolić</i>	
Cycle Slicer: An Algorithm for Building Permutations on Special Domains.	392
<i>Sarah Miracle and Scott Yilek</i>	
Symmetrically and Asymmetrically Hard Cryptography	417
<i>Alex Biryukov and Léo Perrin</i>	
Blockcipher-Based MACs: Beyond the Birthday Bound Without Message Length	446
<i>Yusuke Naito</i>	
Author Index	471

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 I

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

2017, XXVI, 813 p. 121 illus., Softcover

ISBN: 978-3-319-70693-1