

# Contents – Part I

## Best Paper and Honorable Mentions

Tightly CCA-Secure Encryption Without Pairings . . . . .	1
<i>Romain Gay, Dennis Hofheinz, Eike Kiltz, and Hoeteck Wee</i>	
Indistinguishability Obfuscation from Constant-Degree Graded Encoding Schemes . . . . .	28
<i>Huijia Lin</i>	
Essentially Optimal Robust Secret Sharing with Maximal Corruptions . . . . .	58
<i>Allison Bishop, Valerio Pastro, Rajmohan Rajaraman, and Daniel Wichs</i>	

## (Pseudo) Randomness

Provably Robust Sponge-Based PRNGs and KDFs . . . . .	87
<i>Peter Gaži and Stefano Tessaro</i>	
Reusable Fuzzy Extractors for Low-Entropy Distributions . . . . .	117
<i>Ran Canetti, Benjamin Fuller, Omer Paneth, Leonid Reyzin, and Adam Smith</i>	

## LPN/LWE

Provably Weak Instances of Ring-LWE Revisited . . . . .	147
<i>Wouter Castryck, Ilia Iliashenko, and Frederik Vercauteren</i>	
Faster Algorithms for Solving LPN . . . . .	168
<i>Bin Zhang, Lin Jiao, and Mingsheng Wang</i>	

## Cryptanalysis I

Provable Security Evaluation of Structures Against Impossible Differential and Zero Correlation Linear Cryptanalysis. . . . .	196
<i>Bing Sun, Meicheng Liu, Jian Guo, Vincent Rijmen, and Ruilin Li</i>	
Polytopic Cryptanalysis . . . . .	214
<i>Tyge Tiessen</i>	

## Masking

From Improved Leakage Detection to the Detection of Points of Interests in Leakage Traces . . . . .	240
<i>François Durvaux and François-Xavier Standaert</i>	

Improved Masking for Tweakable Blockciphers with Applications to Authenticated Encryption . . . . .	263
<i>Robert Granger, Philipp Jovanovic, Bart Mennink, and Samuel Neves</i>	

## Fully Homomorphic Encryption

Sanitization of FHE Ciphertexts . . . . .	294
<i>Léo Ducas and Damien Stehlé</i>	

Towards Stream Ciphers for Efficient FHE with Low-Noise Ciphertexts . . . .	311
<i>Pierrick Méaux, Anthony Journault, François-Xavier Standaert, and Claude Carlet</i>	

## Cryptanalysis II

Improved Differential-Linear Cryptanalysis of 7-Round Chaskey with Partitioning . . . . .	344
<i>Gaëtan Leurent</i>	

Reverse-Engineering the S-Box of Streebog, Kuznyechik and STRIBOBr1 . . .	372
<i>Alex Biryukov, Léo Perrin, and Aleksei Udovenko</i>	

## Number Theory

Complete Addition Formulas for Prime Order Elliptic Curves. . . . .	403
<i>Joost Renes, Craig Costello, and Lejla Batina</i>	

New Complexity Trade-Offs for the (Multiple) Number Field Sieve Algorithm in Non-Prime Fields . . . . .	429
<i>Palash Sarkar and Shashank Singh</i>	

## Hash Functions

Freestart Collision for Full SHA-1. . . . .	459
<i>Marc Stevens, Pierre Karpman, and Thomas Peyrin</i>	

New Attacks on the Concatenation and XOR Hash Combiners . . . . .	484
<i>Itai Dinur</i>	

**Multilinear Maps**

Cryptanalysis of the New CLT Multilinear Map over the Integers . . . . .	509
<i>Jung Hee Cheon, Pierre-Alain Fouque, Changmin Lee, Brice Minaud, and Hansol Ryu</i>	
Cryptanalysis of GGH Map . . . . .	537
<i>Yupu Hu and Huiwen Jia</i>	

**Message Authentication Codes**

Hash-Function Based PRFs: AMAC and Its Multi-User Security. . . . .	566
<i>Mihir Bellare, Daniel J. Bernstein, and Stefano Tessaro</i>	
On the Influence of Message Length in PMAC’s Security Bounds . . . . .	596
<i>Atul Luykx, Bart Preneel, Alan Szepieniec, and Kan Yasuda</i>	

**Attacks on SSL/TLS**

Lucky Microseconds: A Timing Attack on Amazon’s <i>s2n</i> Implementation of TLS . . . . .	622
<i>Martin R. Albrecht and Kenneth G. Paterson</i>	
An Analysis of OpenSSL’s Random Number Generator . . . . .	644
<i>Falko Strenzke</i>	

**Real-World Protocols**

Safely Exporting Keys from Secure Channels: On the Security of EAP-TLS and TLS Key Exporters. . . . .	670
<i>Christina Brzuska, Håkon Jacobsen, and Douglas Stebila</i>	
Valiant’s Universal Circuit is Practical. . . . .	699
<i>Ágnes Kiss and Thomas Schneider</i>	

**Robust Designs**

Nonce-Based Cryptography: Retaining Security When Randomness Fails. . . .	729
<i>Mihir Bellare and Björn Tackmann</i>	
Honey Encryption Beyond Message Recovery Security . . . . .	758
<i>Joseph Jaeger, Thomas Ristenpart, and Qiang Tang</i>	

**Lattice Reduction**

Improved Progressive BKZ Algorithms and Their Precise Cost Estimation by Sharp Simulator . . . . .	789
<i>Yoshinori Aono, Yuntao Wang, Takuya Hayashi, and Tsuyoshi Takagi</i>	
Practical, Predictable Lattice Basis Reduction . . . . .	820
<i>Daniele Micciancio and Michael Walter</i>	
<b>Author Index</b> . . . . .	851

# Contents – Part II

## Lattice-Based Schemes

Zero-Knowledge Arguments for Lattice-Based Accumulators: Logarithmic-Size Ring Signatures and Group Signatures Without Trapdoors . . . . .	1
<i>Benoît Libert, San Ling, Khoa Nguyen, and Huaxiong Wang</i>	
Adaptively Secure Identity-Based Encryption from Lattices with Asymptotically Shorter Public Parameters . . . . .	32
<i>Shota Yamada</i>	

## Zero-Knowledge I

Online/Offline OR Composition of Sigma Protocols . . . . .	63
<i>Michele Ciampi, Giuseppe Persiano, Alessandra Scafuro, Luisa Siniscalchi, and Ivan Visconti</i>	
Constant-Round Leakage-Resilient Zero-Knowledge from Collision Resistance. . . . .	93
<i>Susumu Kiyoshima</i>	

## Pseudorandom Functions

Constrained Pseudorandom Functions for Unconstrained Inputs . . . . .	124
<i>Apoorva Deshpande, Venkata Koppula, and Brent Waters</i>	
Pseudorandom Functions in Almost Constant Depth from Low-Noise LPN. . .	154
<i>Yu Yu and John Steinberger</i>	

## Multi-Party Computation I

Secure Computation from Elastic Noisy Channels . . . . .	184
<i>Dakshita Khurana, Hemanta K. Maji, and Amit Sahai</i>	
All Complete Functionalities are Reversible . . . . .	213
<i>Dakshita Khurana, Daniel Kraschewski, Hemanta K. Maji, Manoj Prabhakaran, and Amit Sahai</i>	

**Separations**

On the Power of Hierarchical Identity-Based Encryption . . . . .	243
<i>Mohammad Mahmoody and Ameer Mohammed</i>	
On the Impossibility of Tight Cryptographic Reductions . . . . .	273
<i>Christoph Bader, Tibor Jager, Yong Li, and Sven Schäge</i>	

**Zero-Knowledge II**

On the Size of Pairing-Based Non-interactive Arguments . . . . .	305
<i>Jens Groth</i>	
Efficient Zero-Knowledge Arguments for Arithmetic Circuits in the Discrete Log Setting . . . . .	327
<i>Jonathan Bootle, Andrea Cerulli, Pyrros Chaidos, Jens Groth, and Christophe Petit</i>	

**Protocols**

On the Complexity of Script and Proofs of Space in the Parallel Random Oracle Model . . . . .	358
<i>Joël Alwen, Binyi Chen, Chethan Kamath, Vladimir Kolmogorov, Krzysztof Pietrzak, and Stefano Tessaro</i>	
Anonymous Traitor Tracing: How to Embed Arbitrary Information in a Key . . . . .	388
<i>Ryo Nishimaki, Daniel Wichs, and Mark Zhandry</i>	

**Round Complexity**

Unconditionally Secure Computation with Reduced Interaction . . . . .	420
<i>Ivan Damgård, Jesper Buus Nielsen, Rafail Ostrovsky, and Adi Rosén</i>	
The Exact Round Complexity of Secure Computation . . . . .	448
<i>Sanjam Garg, Pratyay Mukherjee, Omkant Pandey, and Antigoni Polychroniadou</i>	

**Commitments**

On the Composition of Two-Prover Commitments, and Applications to Multi-round Relativistic Commitments . . . . .	477
<i>Serge Fehr and Max Fillinger</i>	
Computationally Binding Quantum Commitments . . . . .	497
<i>Dominique Unruh</i>	

**Lattices**

Structural Lattice Reduction: Generalized Worst-Case to Average-Case Reductions and Homomorphic Cryptosystems. . . . .	528
<i>Nicolas Gama, Malika Izabachène, Phong Q. Nguyen, and Xiang Xie</i>	
Recovering Short Generators of Principal Ideals in Cyclotomic Rings . . . . .	559
<i>Ronald Cramer, Léo Ducas, Chris Peikert, and Oded Regev</i>	

**Leakage**

Circuit Compilers with $O(1/\log(n))$ Leakage Rate . . . . .	586
<i>Marcin Andrychowicz, Stefan Dziembowski, and Sebastian Faust</i>	
Randomness Complexity of Private Circuits for Multiplication . . . . .	616
<i>Sonia Belaïd, Fabrice Benhamouda, Alain Passelègue, Emmanuel Prouff, Adrian Thillard, and Damien Vergnaud</i>	

**Indifferentiability**

10-Round Feistel is Indifferentiable from an Ideal Cipher. . . . .	649
<i>Dana Dachman-Soled, Jonathan Katz, and Aishwarya Thiruvengadam</i>	
Indifferentiability of Confusion-Diffusion Networks. . . . .	679
<i>Yevgeniy Dodis, Martijn Stam, John Steinberger, and Tianren Liu</i>	

**Multi-Party Computation II**

Fair and Robust Multi-party Computation Using a Global Transaction Ledger . . . . .	705
<i>Aggelos Kiayias, Hong-Sheng Zhou, and Vassilis Zikas</i>	
Two Round Multiparty Computation via Multi-key FHE . . . . .	735
<i>Pratyay Mukherjee and Daniel Wichs</i>	

**Obfuscation**

Post-zeroizing Obfuscation: New Mathematical Tools, and the Case of Evasive Circuits . . . . .	764
<i>Saikrishna Badrinarayanan, Eric Miles, Amit Sahai, and Mark Zhandry</i>	
New Negative Results on Differing-Inputs Obfuscation . . . . .	792
<i>Mihir Bellare, Igors Stepanovs, and Brent Waters</i>	

**Automated Analysis, Functional Encryption, and Non-malleable Codes**

Automated Unbounded Analysis of Cryptographic Constructions  
in the Generic Group Model. . . . . 822  
*Miguel Ambrona, Gilles Barthe, and Benedikt Schmidt*

Multi-input Functional Encryption in the Private-Key Setting: Stronger  
Security from Weaker Assumptions. . . . . 852  
*Zvika Brakerski, Ilan Komargodski, and Gil Segev*

Non-malleable Codes for Bounded Depth, Bounded Fan-In Circuits . . . . . 881  
*Marshall Ball, Dana Dachman-Soled, Mukul Kulkarni, and Tal Malkin*

**Author Index** . . . . . 909



Advances in Cryptology – EUROCRYPT 2016  
35th Annual International Conference on the Theory  
and Applications of Cryptographic Techniques, Vienna,  
Austria, May 8–12, 2016, Proceedings, Part I  
Fischlin, M.; Coron, J.-S. (Eds.)  
2016, XXVIII, 853 p. 155 illus., Softcover  
ISBN: 978-3-662-49889-7