

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>Apoorvaa 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
<i>Miguel Ambrona, Gilles Barthe, and Benedikt Schmidt</i>	
Multi-input Functional Encryption in the Private-Key Setting: Stronger Security from Weaker Assumptions.	852
<i>Zvika Brakerski, Ilan Komargodski, and Gil Segev</i>	
Non-malleable Codes for Bounded Depth, Bounded Fan-In Circuits	881
<i>Marshall Ball, Dana Dachman-Soled, Mukul Kulkarni, and Tal Malkin</i>	
Author Index	909