Contents – Part II

Delegation and IP

Delegating RAM Computations with Adaptive Soundness and Privacy 3
Prabhanjan Ananth, Yu-Chi Chen, Kai-Min Chung, Huijia Lin, and Wei-Kai Lin

Interactive Oracle Proofs 31
Eli Ben-Sasson, Alessandro Chiesa, and Nicholas Spooner

Adaptive Succinct Garbled RAM or: How to Delegate Your Database..... 61
Ran Canetti, Yilei Chen, Justin Holmgren, and Mariana Raykova

Delegating RAM Computations 91
Yael Kalai and Omer Paneth

Public-Key Encryption

Standard Security Does Not Imply Indistinguishability Under Selective Opening..... 121
Dennis Hofheinz, Vanishree Rao, and Daniel Wichs

Public-Key Encryption with Simulation-Based Selective-Opening Security and Compact Ciphertexts 146
Dennis Hofheinz, Tibor Jager, and Andy Rupp

Towards Non-Black-Box Separations of Public Key Encryption and One Way Function..... 169
Dana Dachman-Soled

Post-Quantum Security of the Fujisaki-Okamoto and OAEP Transforms 192
Ehsan Ebrahimi Targhi and Dominique Unruh

Multi-key FHE from LWE, Revisited 217
Chris Peikert and Sina Shiehian

Obfuscation and Multilinear Maps

Secure Obfuscation in a Weak Multilinear Map Model 241
Sanjam Garg, Eric Miles, Pratyay Mukherjee, Amit Sahai, Akshayaram Srinivasan, and Mark Zhandry

Virtual Grey-Boxes Beyond Obfuscation: A Statistical Security Notion for Cryptographic Agents . . . 269
Shashank Agrawal, Manoj Prabhakaran, and Ching-Hua Yu

Attribute-Based Encryption

Deniable Attribute Based Encryption for Branching Programs from LWE . . . 299
Daniel Apon, Xiong Fan, and Feng-Hao Liu

Targeted Homomorphic Attribute-Based Encryption . . . 330
Zvika Brakerski, David Cash, Rotem Tsabary, and Hoeteck Wee

Semi-adaptive Security and Bundling Functionalities Made Generic and Easy . . . 361
Rishab Goyal, Venkata Koppula, and Brent Waters

Functional Encryption

From Cryptomania to Obfustopia Through Secret-Key Functional Encryption . . . 391
Nir Bitansky, Ryo Nishimaki, Alain Passelègue, and Daniel Wichs

Single-Key to Multi-Key Functional Encryption with Polynomial Loss . . . 419
Sanjam Garg and Akshayaram Srinivasan

Compactness vs Collusion Resistance in Functional Encryption . . . 443
Baiyu Li and Daniele Micciancio

Secret Sharing

Threshold Secret Sharing Requires a Linear Size Alphabet . . . 471
Andrej Bogdanov, Siyao Guo, and Ilan Komargodski

How to Share a Secret, Infinitely . . . 485
Ilan Komargodski, Moni Naor, and Eylon Yogev

New Models

Designing Proof of Human-Work Puzzles for Cryptocurrency and Beyond . . . 517
Jeremiah Blocki and Hong-Sheng Zhou

Access Control Encryption: Enforcing Information Flow with Cryptography . . . 547
Ivan Damgård, Helene Haagh, and Claudio Orlandi

Author Index . . . 577

Contents – Part I

TCC Test-of-Time Award

From Indifferentiability to Constructive Cryptography (and Back) 3
Ueli Maurer and Renato Renner

Foundations

Fast Pseudorandom Functions Based on Expander Graphs 27
Benny Applebaum and Pavel Raykov

3-Message Zero Knowledge Against Human Ignorance 57
Nir Bitansky, Zvika Brakerski, Yael Kalai, Omer Paneth, and Vinod Vaikuntanathan

The GGM Function Family Is a Weakly One-Way Family of Functions 84
Aloni Cohen and Saleet Klein

On the (In)Security of SNARKs in the Presence of Oracles 108
Dario Fiore and Anca Nitulescu

Leakage Resilient One-Way Functions: The Auxiliary-Input Setting 139
Ilan Komargodski

Simulating Auxiliary Inputs, Revisited 159
Maciej Skórski

Unconditional Security

Pseudoentropy: Lower-Bounds for Chain Rules and Transformations 183
Krzysztof Pietrzak and Maciej Skórski

Oblivious Transfer from Any Non-trivial Elastic Noisy Channel via Secret Key Agreement 204
Ignacio Cascudo, Ivan Damgård, Felipe Lacerda, and Samuel Ranellucci

Simultaneous Secrecy and Reliability Amplification for a General Channel Model 235
Russell Impagliazzo, Ragesh Jaiswal, Valentine Kabanets, Bruce M. Kapron, Valerie King, and Stefano Tessaro

Proof of Space from Stacked Expanders 262
Ling Ren and Srinivas Devadas

Perfectly Secure Message Transmission in Two Rounds 286
Gabriele Spini and Gilles Zémor

Foundations of Multi-Party Protocols

Almost-Optimally Fair Multiparty Coin-Tossing with Nearly Three-Quarters Malicious 307
Bar Alon and Eran Omri

Binary AMD Circuits from Secure Multiparty Computation 336
Daniel Genkin, Yuval Ishai, and Mor Weiss

Composable Security in the Tamper-Proof Hardware Model Under Minimal Complexity 367
Carmit Hazay, Antigoni Polychroniadou, and Muthuramakrishnan Venkitasubramaniam

Composable Adaptive Secure Protocols Without Setup Under Polytime Assumptions 400
Carmit Hazay and Muthuramakrishnan Venkitasubramaniam

Adaptive Security of Yao's Garbled Circuits 433
Zahra Jafargholi and Daniel Wichs

Round Complexity and Efficiency of Multi-party Computation

Efficient Secure Multiparty Computation with Identifiable Abort 461
Carsten Baum, Emmanuela Orsini, and Peter Scholl

Secure Multiparty RAM Computation in Constant Rounds 491
Sanjam Garg, Divya Gupta, Peihan Miao, and Omkant Pandey

Constant-Round Maliciously Secure Two-Party Computation in the RAM Model 521
Carmit Hazay and Avishay Yanai

More Efficient Constant-Round Multi-party Computation from BMR and SHE 554
Yehuda Lindell, Nigel P. Smart, and Eduardo Soria-Vazquez

Cross and Clean: Amortized Garbled Circuits with Constant Overhead 582
Jesper Buus Nielsen and Claudio Orlandi

Differential Privacy

Separating Computational and Statistical Differential Privacy in the Client-Server Model 607
Mark Bun, Yi-Hsiu Chen, and Salil Vadhan

Concentrated Differential Privacy: Simplifications, Extensions, and Lower Bounds 635
Mark Bun and Thomas Steinke

Strong Hardness of Privacy from Weak Traitor Tracing 659
Lucas Kowalczyk, Tal Malkin, Jonathan Ullman, and Mark Zhandry

Author Index 691

http://www.springer.com/978-3-662-53643-8

Theory of Cryptography
14th International Conference, TCC 2016-B, Beijing, China, October 31-November 3, 2016, Proceedings, Part II
Hirt, M.; Smith, A. (Eds.)
2016, XV, 578 p. 32 illus., Softcover
ISBN: 978-3-662-53643-8