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