

Contents – Part I

TCC Test-of-Time Award

From Indifferentiability to Constructive Cryptography (and Back)	3
<i>Ueli Maurer and Renato Renner</i>	

Foundations

Fast Pseudorandom Functions Based on Expander Graphs	27
<i>Benny Applebaum and Pavel Raykov</i>	
3-Message Zero Knowledge Against Human Ignorance	57
<i>Nir Bitansky, Zvika Brakerski, Yael Kalai, Omer Paneth, and Vinod Vaikuntanathan</i>	
The GGM Function Family Is a Weakly One-Way Family of Functions	84
<i>Aloni Cohen and Saleet Klein</i>	
On the (In)Security of SNARKs in the Presence of Oracles	108
<i>Dario Fiore and Anca Nitulescu</i>	
Leakage Resilient One-Way Functions: The Auxiliary-Input Setting	139
<i>Ilan Komargodski</i>	
Simulating Auxiliary Inputs, Revisited	159
<i>Maciej Skórski</i>	

Unconditional Security

Pseudoentropy: Lower-Bounds for Chain Rules and Transformations.	183
<i>Krzysztof Pietrzak and Maciej Skórski</i>	
Oblivious Transfer from Any Non-trivial Elastic Noisy Channel via Secret Key Agreement.	204
<i>Ignacio Cascudo, Ivan Damgård, Felipe Lacerda, and Samuel Ranellucci</i>	
Simultaneous Secrecy and Reliability Amplification for a General Channel Model	235
<i>Russell Impagliazzo, Ragesh Jaiswal, Valentine Kabanets, Bruce M. Kapron, Valerie King, and Stefano Tessaro</i>	

Proof of Space from Stacked Expanders.	262
<i>Ling Ren and Srinivas Devadas</i>	

Perfectly Secure Message Transmission in Two Rounds.	286
<i>Gabriele Spini and Gilles Zémor</i>	

Foundations of Multi-Party Protocols

Almost-Optimally Fair Multiparty Coin-Tossing with Nearly Three-Quarters Malicious.	307
<i>Bar Alon and Eran Omri</i>	

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

Composable Security in the Tamper-Proof Hardware Model Under Minimal Complexity	367
<i>Carmit Hazay, Antigoni Polychroniadou, and Muthuramakrishnan Venkatasubramanian</i>	

Composable Adaptive Secure Protocols Without Setup Under Polytime Assumptions.	400
<i>Carmit Hazay and Muthuramakrishnan Venkatasubramanian</i>	

Adaptive Security of Yao’s Garbled Circuits	433
<i>Zahra Jafargholi and Daniel Wichs</i>	

Round Complexity and Efficiency of Multi-party Computation

Efficient Secure Multiparty Computation with Identifiable Abort.	461
<i>Carsten Baum, Emmanuela Orsini, and Peter Scholl</i>	

Secure Multiparty RAM Computation in Constant Rounds.	491
<i>Sanjam Garg, Divya Gupta, Peihan Miao, and Omkant Pandey</i>	

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

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

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

Differential Privacy

Separating Computational and Statistical Differential Privacy in the Client-Server Model	607
<i>Mark Bun, Yi-Hsiu Chen, and Salil Vadhan</i>	
Concentrated Differential Privacy: Simplifications, Extensions, and Lower Bounds	635
<i>Mark Bun and Thomas Steinke</i>	
Strong Hardness of Privacy from Weak Traitor Tracing	659
<i>Lucas Kowalczyk, Tal Malkin, Jonathan Ullman, and Mark Zhandry</i>	
Author Index	691

Contents – Part II

Delegation and IP

Delegating RAM Computations with Adaptive Soundness and Privacy	3
<i>Prabhanjan Ananth, Yu-Chi Chen, Kai-Min Chung, Huijia Lin, and Wei-Kai Lin</i>	
Interactive Oracle Proofs	31
<i>Eli Ben-Sasson, Alessandro Chiesa, and Nicholas Spooner</i>	
Adaptive Succinct Garbled RAM or: How to Delegate Your Database.	61
<i>Ran Canetti, Yilei Chen, Justin Holmgren, and Mariana Raykova</i>	
Delegating RAM Computations	91
<i>Yael Kalai and Omer Paneth</i>	

Public-Key Encryption

Standard Security Does Not Imply Indistinguishability Under Selective Opening.	121
<i>Dennis Hofheinz, Vanishree Rao, and Daniel Wichs</i>	
Public-Key Encryption with Simulation-Based Selective-Opening Security and Compact Ciphertexts	146
<i>Dennis Hofheinz, Tibor Jager, and Andy Rupp</i>	
Towards Non-Black-Box Separations of Public Key Encryption and One Way Function.	169
<i>Dana Dachman-Soled</i>	
Post-Quantum Security of the Fujisaki-Okamoto and OAEP Transforms	192
<i>Ehsan Ebrahimi Targhi and Dominique Unruh</i>	
Multi-key FHE from LWE, Revisited	217
<i>Chris Peikert and Sina Shiehian</i>	

Obfuscation and Multilinear Maps

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

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

Attribute-Based Encryption

Deniable Attribute Based Encryption for Branching Programs from LWE . . .	299
<i>Daniel Apon, Xiong Fan, and Feng-Hao Liu</i>	
Targeted Homomorphic Attribute-Based Encryption	330
<i>Zvika Brakerski, David Cash, Rotem Tsabary, and Hoeteck Wee</i>	
Semi-adaptive Security and Bundling Functionalities Made Generic and Easy	361
<i>Rishab Goyal, Venkata Koppula, and Brent Waters</i>	

Functional Encryption

From Cryptomania to Obfustopia Through Secret-Key Functional Encryption	391
<i>Nir Bitansky, Ryo Nishimaki, Alain Passelègue, and Daniel Wichs</i>	
Single-Key to Multi-Key Functional Encryption with Polynomial Loss	419
<i>Sanjam Garg and Akshayaram Srinivasan</i>	
Compactness vs Collusion Resistance in Functional Encryption	443
<i>Baiyu Li and Daniele Micciancio</i>	

Secret Sharing

Threshold Secret Sharing Requires a Linear Size Alphabet	471
<i>Andrej Bogdanov, Siyao Guo, and Ilan Komargodski</i>	
How to Share a Secret, Infinitely	485
<i>Ilan Komargodski, Moni Naor, and Eylon Yogev</i>	

New Models

Designing Proof of Human-Work Puzzles for Cryptocurrency and Beyond. . .	517
<i>Jeremiah Blocki and Hong-Sheng Zhou</i>	
Access Control Encryption: Enforcing Information Flow with Cryptography	547
<i>Ivan Damgård, Helene Haagh, and Claudio Orlandi</i>	

Author Index	577
-------------------------------	-----

Theory of Cryptography

14th International Conference, TCC 2016-B, Beijing,
China, October 31-November 3, 2016, Proceedings,
Part I

Hirt, M.; Smith, A. (Eds.)

2016, XVI, 692 p. 85 illus., Softcover

ISBN: 978-3-662-53640-7