

# Contents – Part I

## Impossibilities and Barriers

Barriers to Black-Box Constructions of Traitor Tracing Systems . . . . .	3
<i>Bo Tang and Jiapeng Zhang</i>	
On the Impossibility of Entropy Reversal, and Its Application to Zero-Knowledge Proofs . . . . .	31
<i>Shachar Lovett and Jiapeng Zhang</i>	
Position-Based Cryptography and Multiparty Communication Complexity . . .	56
<i>Joshua Brody, Stefan Dziembowski, Sebastian Faust, and Krzysztof Pietrzak</i>	
When Does Functional Encryption Imply Obfuscation? . . . . .	82
<i>Sanjam Garg, Mohammad Mahmoody, and Ameer Mohammed</i>	

## Obfuscation

Limits on the Locality of Pseudorandom Generators and Applications to Indistinguishability Obfuscation. . . . .	119
<i>Alex Lombardi and Vinod Vaikuntanathan</i>	
Decomposable Obfuscation: A Framework for Building Applications of Obfuscation from Polynomial Hardness . . . . .	138
<i>Qipeng Liu and Mark Zhandry</i>	

## Functional Encryption

Functional Encryption for Bounded Collusions, Revisited. . . . .	173
<i>Shweta Agrawal and Alon Rosen</i>	
Attribute-Hiding Predicate Encryption in Bilinear Groups, Revisited . . . . .	206
<i>Hoeteck Wee</i>	

## Constrained PRFs

Constrained Keys for Invertible Pseudorandom Functions. . . . .	237
<i>Dan Boneh, Sam Kim, and David J. Wu</i>	
Private Constrained PRFs (and More) from LWE . . . . .	264
<i>Zvika Brakerski, Rotem Tsabary, Vinod Vaikuntanathan, and Hoeteck Wee</i>	

## Encryption

The Edited Truth. . . . .	305
<i>Shafi Goldwasser, Saleet Klein, and Daniel Wichs</i>	
A Modular Analysis of the Fujisaki-Okamoto Transformation. . . . .	341
<i>Dennis Hofheinz, Kathrin Hövelmanns, and Eike Kiltz</i>	
From Selective IBE to Full IBE and Selective HIBE . . . . .	372
<i>Nico Döttling and Sanjam Garg</i>	
Multi-key Authenticated Encryption with Corruptions: Reductions Are Lossy . . . . .	409
<i>Tibor Jager, Martijn Stam, Ryan Stanley-Oakes, and Bogdan Warinschi</i>	

## Moderately Hard Functions

On the Depth-Robustness and Cumulative Pebbling Cost of Argon2i. . . . .	445
<i>Jeremiah Blocki and Samson Zhou</i>	
Bandwidth Hard Functions for ASIC Resistance . . . . .	466
<i>Ling Ren and Srinivas Devadas</i>	
Moderately Hard Functions: Definition, Instantiations, and Applications. . . . .	493
<i>Joël Alwen and Björn Tackmann</i>	

## Blockchains

Overcoming Cryptographic Impossibility Results Using Blockchains . . . . .	529
<i>Rishab Goyal and Vipul Goyal</i>	

## Multiparty Computation

Secure Two-Party Computation with Fairness - A Necessary Design Principle . . . . .	565
<i>Yehuda Lindell and Tal Rabin</i>	
Designing Fully Secure Protocols for Secure Two-Party Computation of Constant-Domain Functions . . . . .	581
<i>Vanesa Daza and Nikolaos Makriyannis</i>	
On Secure Two-Party Computation in Three Rounds. . . . .	612
<i>Prabhanjan Ananth and Abhishek Jain</i>	
Four Round Secure Computation Without Setup . . . . .	645
<i>Zvika Brakerski, Shai Halevi, and Antigoni Polychroniadou</i>	

Round-Optimal Secure Two-Party Computation from Trapdoor Permutations . . . . .	678
<i>Michele Ciampi, Rafail Ostrovsky, Luisa Siniscalchi, and Ivan Visconti</i>	
Delayed-Input Non-Malleable Zero Knowledge and Multi-Party Coin Tossing in Four Rounds . . . . .	711
<i>Michele Ciampi, Rafail Ostrovsky, Luisa Siniscalchi, and Ivan Visconti</i>	
Round Optimal Concurrent MPC via Strong Simulation . . . . .	743
<i>Saikrishna Badrinarayanan, Vipul Goyal, Abhishek Jain, Dakshita Khurana, and Amit Sahai</i>	
A Unified Approach to Constructing Black-Box UC Protocols in Trusted Setup Models . . . . .	776
<i>Susumu Kiyoshima, Huijia Lin, and Muthuramakrishnan Venkatasubramaniam</i>	
<b>Author Index . . . . .</b>	<b>811</b>

## Contents – Part II

### Garbled Circuits and Oblivious RAM

Actively Secure Garbled Circuits with Constant Communication Overhead in the Plain Model . . . . .	3
<i>Carmit Hazay, Yuval Ishai, and Muthuramakrishnan Venkatasubramanian</i>	
Adaptively Indistinguishable Garbled Circuits . . . . .	40
<i>Zahra Jafargholi, Alessandra Scafuro, and Daniel Wichs</i>	
Circuit OPRAM: Unifying Statistically and Computationally Secure ORAMs and OPRAMs . . . . .	72
<i>T.-H. Hubert Chan and Elaine Shi</i>	

### Zero-Knowledge and Non-Malleability

Resettably-Sound Resetable Zero Knowledge in Constant Rounds . . . . .	111
<i>Wutichai Chongchitmate, Rafail Ostrovsky, and Ivan Visconti</i>	
Round Optimal Concurrent Non-malleability from Polynomial Hardness . . . .	139
<i>Dakshita Khurana</i>	
Zero Knowledge Protocols from Succinct Constraint Detection . . . . .	172
<i>Eli Ben-Sasson, Alessandro Chiesa, Michael A. Forbes, Ariel Gabizon, Michael Riabzev, and Nicholas Spooner</i>	

### Leakage and Tampering

How to Construct a Leakage-Resilient (Stateless) Trusted Party . . . . .	209
<i>Daniel Genkin, Yuval Ishai, and Mor Weiss</i>	
Blockwise $p$ -Tampering Attacks on Cryptographic Primitives, Extractors, and Learners. . . . .	245
<i>Saeed Mahloujifar and Mohammad Mahmoody</i>	

### Delegation

On Zero-Testable Homomorphic Encryption and Publicly Verifiable Non-interactive Arguments . . . . .	283
<i>Omer Paneth and Guy N. Rothblum</i>	

## Non-Malleable Codes

Inception Makes Non-malleable Codes Stronger . . . . .	319
<i>Divesh Aggarwal, Tomasz Kazana, and Maciej Obremski</i>	
Four-State Non-malleable Codes with Explicit Constant Rate . . . . .	344
<i>Bhavana Kanukurthi, Sai Lakshmi Bhavana Obbattu, and Sruthi Sekar</i>	

## Secret Sharing

Evolving Secret Sharing: Dynamic Thresholds and Robustness . . . . .	379
<i>Ilan Komargodski and Anat Paskin-Cherniavsky</i>	
Linear Secret-Sharing Schemes for Forbidden Graph Access Structures . . . . .	394
<i>Amos Beimel, Oriol Farràs, Yuval Mintz, and Naty Peter</i>	
Near-Optimal Secret Sharing and Error Correcting Codes in $AC^0$ . . . . .	424
<i>Kuan Cheng, Yuval Ishai, and Xin Li</i>	

## OT Combiners

Resource-Efficient OT Combiners with Active Security . . . . .	461
<i>Ignacio Cascudo, Ivan Damgård, Oriol Farràs, and Samuel Ranellucci</i>	

## Signatures

An Equivalence Between Attribute-Based Signatures and Homomorphic Signatures, and New Constructions for Both. . . . .	489
<i>Rotem Tsabary</i>	
On the One-Per-Message Unforgeability of (EC)DSA and Its Variants. . . . .	519
<i>Manuel Ferssch, Eike Kiltz, and Bertram Poettering</i>	

## Verifiable Random Functions

A Generic Approach to Constructing and Proving Verifiable Random Functions . . . . .	537
<i>Rishab Goyal, Susan Hohenberger, Venkata Koppula, and Brent Waters</i>	
Verifiable Random Functions from Non-interactive Witness-Indistinguishable Proofs . . . . .	567
<i>Nir Bitansky</i>	

## Fully Homomorphic Encryption

Batched Multi-hop Multi-key FHE from Ring-LWE with Compact Ciphertext Extension . . . . .	597
<i>Long Chen, Zhenfeng Zhang, and Xueqing Wang</i>	

**Database Privacy**

Strengthening the Security of Encrypted Databases: Non-transitive JOINS . . .	631
<i>Ilya Mironov, Gil Segev, and Ido Shahaf</i>	
Can We Access a Database Both Locally and Privately? . . . . .	662
<i>Elette Boyle, Yuval Ishai, Rafael Pass, and Mary Wootters</i>	
Towards Doubly Efficient Private Information Retrieval. . . . .	694
<i>Ran Canetti, Justin Holmgren, and Silas Richelson</i>	

**Assumptions**

On Iterative Collision Search for LPN and Subset Sum . . . . .	729
<i>Srinivas Devadas, Ling Ren, and Hanshen Xiao</i>	
Can PPAD Hardness be Based on Standard Cryptographic Assumptions? . . .	747
<i>Alon Rosen, Gil Segev, and Ido Shahaf</i>	

<b>Author Index</b> . . . . .	777
-------------------------------	-----

Theory of Cryptography

15th International Conference, TCC 2017, Baltimore,  
MD, USA, November 12-15, 2017, Proceedings, Part I

Tauman Kalai, Y.; Reyzin, L. (Eds.)

2017, XVII, 812 p. 80 illus., Softcover

ISBN: 978-3-319-70499-9