

Contents – Part II

OT and ORAM

Secure Computation Based on Leaky Correlations: High Resilience Setting . . .	3
<i>Alexander R. Block, Hemanta K. Maji, and Hai H. Nguyen</i>	
Laconic Oblivious Transfer and Its Applications	33
<i>Chongwon Cho, Nico Döttling, Sanjam Garg, Divya Gupta, Peihan Miao, and Antigoni Polychroniadou</i>	
Black-Box Parallel Garbled RAM	66
<i>Steve Lu and Rafail Ostrovsky</i>	

Foundations II

Non-Malleable Codes for Space-Bounded Tampering	95
<i>Sebastian Faust, Kristina Hostáková, Pratyay Mukherjee, and Daniele Venturi</i>	
Four-Round Concurrent Non-Malleable Commitments from One-Way Functions	127
<i>Michele Ciampi, Rafail Ostrovsky, Luisa Siniscalchi, and Ivan Visconti</i>	
Distinguisher-Dependent Simulation in Two Rounds and its Applications. . .	158
<i>Abhishek Jain, Yael Tauman Kalai, Dakshita Khurana, and Ron Rothblum</i>	

Obfuscation II

Incremental Program Obfuscation	193
<i>Sanjam Garg and Omkant Pandey</i>	
From Obfuscation to the Security of Fiat-Shamir for Proofs	224
<i>Yael Tauman Kalai, Guy N. Rothblum, and Ron D. Rothblum</i>	
Indistinguishability Obfuscation for Turing Machines: Constant Overhead and Amortization.	252
<i>Prabhanjan Ananth, Abhishek Jain, and Amit Sahai</i>	

Quantum

Quantum Security of NMAC and Related Constructions: PRF Domain Extension Against Quantum attacks.	283
<i>Fang Song and Aaram Yun</i>	
Quantum Non-malleability and Authentication	310
<i>Gorjan Alagic and Christian Majenz</i>	
New Security Notions and Feasibility Results for Authentication of Quantum Data	342
<i>Sumegha Garg, Henry Yuen, and Mark Zhandry</i>	

Hash Functions

Time-Memory Tradeoff Attacks on the MTP Proof-of-Work Scheme.	375
<i>Itai Dinur and Niv Nadler</i>	
Functional Graph Revisited: Updates on (Second) Preimage Attacks on Hash Combiners.	404
<i>Zhenzhen Bao, Lei Wang, Jian Guo, and Dawu Gu</i>	
Non-full Sbox Linearization: Applications to Collision Attacks on Round-Reduced KECCAK	428
<i>Ling Song, Guohong Liao, and Jian Guo</i>	

Lattices

Gaussian Sampling over the Integers: Efficient, Generic, Constant-Time	455
<i>Daniele Micciancio and Michael Walter</i>	
LPN Decoded.	486
<i>Andre Esser, Robert Kübler, and Alexander May</i>	

Signatures

Optimal Security Reductions for Unique Signatures: Bypassing Impossibilities with a Counterexample.	517
<i>Fuchun Guo, Rongmao Chen, Willy Susilo, Jianchang Lai, Guomin Yang, and Yi Mu</i>	
Compact Structure-Preserving Signatures with Almost Tight Security	548
<i>Masayuki Abe, Dennis Hofheinz, Ryo Nishimaki, Miyako Ohkubo, and Jiaxin Pan</i>	

Snarky Signatures: Minimal Signatures of Knowledge from Simulation-Extractable SNARKs	581
<i>Jens Groth and Mary Maller</i>	

Fast Secure Two-Party ECDSA Signing.	613
<i>Yehuda Lindell</i>	

Block Ciphers

Proving Resistance Against Invariant Attacks: How to Choose the Round Constants	647
<i>Christof Beierle, Anne Canteaut, Gregor Leander, and Yann Rotella</i>	

Breaking the FF3 Format-Preserving Encryption Standard over Small Domains	679
<i>F. Betül Durak and Serge Vaudenay</i>	

Insuperability of the Standard Versus Ideal Model Gap for Tweakable Blockcipher Security	708
<i>Bart Mennink</i>	

Author Index	733
-------------------------------	-----

<http://www.springer.com/978-3-319-63714-3>

Advances in Cryptology – CRYPTO 2017
37th Annual International Cryptology Conference, Santa
Barbara, CA, USA, August 20–24, 2017, Proceedings,
Part II
Katz, J.; Shacham, H. (Eds.)
2017, XV, 735 p. 100 illus., Softcover
ISBN: 978-3-319-63714-3