

Contents – Part II

Zero Knowledge and PCP

Making the Best of a Leaky Situation: Zero-Knowledge PCPs from Leakage-Resilient Circuits	3
<i>Yuval Ishai, Mor Weiss, and Guang Yang</i>	
Quasi-Linear Size Zero Knowledge from Linear-Algebraic PCPs.	33
<i>Eli Ben-Sasson, Alessandro Chiesa, Ariel Gabizon, and Madars Virza</i>	
From Private Simultaneous Messages to Zero-Information Arthur-Merlin Protocols and Back	65
<i>Benny Applebaum and Pavel Raykov</i>	
A Transform for NIZK Almost as Efficient and General as the Fiat-Shamir Transform Without Programmable Random Oracles.	83
<i>Michele Ciampi, Giuseppe Persiano, Luisa Siniscalchi, and Ivan Visconti</i>	
Improved OR-Composition of Sigma-Protocols.	112
<i>Michele Ciampi, Giuseppe Persiano, Alessandra Scafuro, Luisa Siniscalchi, and Ivan Visconti</i>	

Oblivious RAM

Onion ORAM: A Constant Bandwidth Blowup Oblivious RAM.	145
<i>Srinivas Devadas, Marten van Dijk, Christopher W. Fletcher, Ling Ren, Elaine Shi, and Daniel Wichs</i>	
Oblivious Parallel RAM and Applications	175
<i>Elette Boyle, Kai-Min Chung, and Rafael Pass</i>	
Oblivious Parallel RAM: Improved Efficiency and Generic Constructions . . .	205
<i>Binyi Chen, Huijia Lin, and Stefano Tessaro</i>	

ABE and IBE

Déjà Q: Encore! Un Petit IBE	237
<i>Hoeteck Wee</i>	
A Study of Pair Encodings: Predicate Encryption in Prime Order Groups. . . .	259
<i>Shashank Agrawal and Melissa Chase</i>	

Codes and Interactive Proofs

Optimal Amplification of Noisy Leakages 291
Stefan Dziembowski, Sebastian Faust, and Maciej Skórski

Rational Sumchecks 319
Siyao Guo, Pavel Hubáček, Alon Rosen, and Margarita Vald

Interactive Coding for Interactive Proofs 352
Allison Bishop and Yevgeniy Dodis

Information-Theoretic Local Non-malleable Codes and Their Applications . . . 367
Nishanth Chandran, Bhavana Kanukurthi, and Srinivasan Raghuraman

Optimal Computational Split-state Non-malleable Codes 393
Divesh Aggarwal, Shashank Agrawal, Divya Gupta, Hemanta K. Maji, Omkant Pandey, and Manoj Prabhakaran

Limitations of Obfuscation and Obfuscation-Avoiding Constructions

How to Avoid Obfuscation Using Witness PRFs. 421
Mark Zhandry

Cutting-Edge Cryptography Through the Lens of Secret Sharing 449
Ilan Komargodski and Mark Zhandry

Functional Encryption Without Obfuscation 480
Sanjam Garg, Craig Gentry, Shai Halevi, and Mark Zhandry

On Constructing One-Way Permutations from Indistinguishability
 Obfuscation 512
Gilad Asharov and Gil Segev

Contention in Cryptoland: Obfuscation, Leakage and UCE. 542
Mihir Bellare, Igors Stepanovs, and Stefano Tessaro

Point-Function Obfuscation: A Framework and Generic Constructions 565
Mihir Bellare and Igors Stepanovs

Author Index 595

Contents – Part I

Obfuscation: Impossibility Results and Constructions

Impossibility of VBB Obfuscation with Ideal Constant-Degree Graded Encodings	3
<i>Rafael Pass and Abhi Shelat</i>	
On the Impossibility of Virtual Black-Box Obfuscation in Idealized Models . . .	18
<i>Mohammad Mahmoody, Ameer Mohammed, and Soheil Nematihaji</i>	
Lower Bounds on Assumptions Behind Indistinguishability Obfuscation	49
<i>Mohammad Mahmoody, Ameer Mohammed, Soheil Nematihaji, Rafael Pass, and Abhi Shelat</i>	
Indistinguishability Obfuscation: From Approximate to Exact	67
<i>Nir Bitansky and Vinod Vaikuntanathan</i>	
Output-Compressing Randomized Encodings and Applications	96
<i>Huijia Lin, Rafael Pass, Karn Seth, and Sidharth Telang</i>	
Functional Encryption for Turing Machines	125
<i>Prabhanjan Ananth and Amit Sahai</i>	

Differential Privacy

The Complexity of Computing the Optimal Composition of Differential Privacy	157
<i>Jack Murtagh and Salil Vadhan</i>	
Order-Revealing Encryption and the Hardness of Private Learning	176
<i>Mark Bun and Mark Zhandry</i>	

LWR and LPN

On the Hardness of Learning with Rounding over Small Modulus	209
<i>Andrej Bogdanov, Siyao Guo, Daniel Masny, Silas Richelson, and Alon Rosen</i>	
Two-Round Man-in-the-Middle Security from LPN	225
<i>David Cash, Eike Kiltz, and Stefano Tessaro</i>	

Public Key Encryption, Signatures, and VRF

Algebraic Partitioning: Fully Compact and (almost) Tightly Secure
 Cryptography 251
Dennis Hofheinz

Standard Security Does Imply Security Against Selective Opening for
 Markov Distributions 282
Georg Fuchsbauer, Felix Heuer, Eike Kiltz, and Krzysztof Pietrzak

Non-Malleable Encryption: Simpler, Shorter, Stronger 306
Sandro Coretti, Yevgeniy Dodis, Björn Tackmann, and Daniele Venturi

Verifiable Random Functions from Standard Assumptions 336
Dennis Hofheinz and Tibor Jager

Complexity of Cryptographic Primitives

Homomorphic Evaluation Requires Depth 365
Andrej Bogdanov and Chin Ho Lee

On Basing Private Information Retrieval on NP-Hardness 372
Tianren Liu and Vinod Vaikuntanathan

Obfuscation-Based Cryptographic Constructions

On the Correlation Intractability of Obfuscated Pseudorandom Functions 389
Ran Canetti, Yilei Chen, and Leonid Reyzin

Reconfigurable Cryptography: A Flexible Approach to Long-Term Security . . . 416
Julia Hesse, Dennis Hofheinz, and Andy Rupp

Multilinear Maps from Obfuscation 446
*Martin R. Albrecht, Pooya Farshim, Dennis Hofheinz, Enrique Larraia,
 and Kenneth G. Paterson*

Perfect Structure on the Edge of Chaos: Trapdoor Permutations from
 Indistinguishability Obfuscation 474
Nir Bitansky, Omer Paneth, and Daniel Wichs

Cryptographic Assumptions (Invited Talk followed by Panel)

Cryptographic Assumptions: A Position Paper 505
Shafi Goldwasser and Yael Tauman Kalai

Multiparty Computation

Adaptive Security with Quasi-Optimal Rate 525
Brett Hemenway, Rafail Ostrovsky, Silas Richelson, and Alon Rosen

On the Complexity of Additively Homomorphic UC Commitments. 542
*Tore Kasper Frederiksen, Thomas P. Jakobsen, Jesper Buus Nielsen,
and Roberto Trifiletti*

Simplified Universal Composability Framework 566
Douglas Wikström

Characterization of Secure Multiparty Computation Without Broadcast 596
Ran Cohen, Iftach Haitner, Eran Omri, and Lior Rotem

Author Index 617



<http://www.springer.com/978-3-662-49098-3>

Theory of Cryptography

13th International Conference, TCC 2016-A, Tel Aviv,

Israel, January 10-13, 2016, Proceedings, Part II

Kushilevitz, E.; Malkin, T. (Eds.)

2016, XIII, 596 p. 63 illus., Softcover

ISBN: 978-3-662-49098-3