

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
<i>Stefan Dziembowski, Sebastian Faust, and Maciej Skórski</i>	
Rational Sumchecks	319
<i>Siyao Guo, Pavel Hubáček, Alon Rosen, and Margarita Vald</i>	
Interactive Coding for Interactive Proofs	352
<i>Allison Bishop and Yevgeniy Dodis</i>	
Information-Theoretic Local Non-malleable Codes and Their Applications . . .	367
<i>Nishanth Chandran, Bhavana Kanukurthi, and Srinivasan Raghuraman</i>	
Optimal Computational Split-state Non-malleable Codes	393
<i>Divesh Aggarwal, Shashank Agrawal, Divya Gupta, Hemanta K. Maji, Omkant Pandey, and Manoj Prabhakaran</i>	

Limitations of Obfuscation and Obfuscation-Avoiding Constructions

How to Avoid Obfuscation Using Witness PRFs.	421
<i>Mark Zhandry</i>	
Cutting-Edge Cryptography Through the Lens of Secret Sharing.	449
<i>Ilan Komargodski and Mark Zhandry</i>	
Functional Encryption Without Obfuscation	480
<i>Sanjam Garg, Craig Gentry, Shai Halevi, and Mark Zhandry</i>	
On Constructing One-Way Permutations from Indistinguishability Obfuscation	512
<i>Gilad Asharov and Gil Segev</i>	
Contention in Cryptoland: Obfuscation, Leakage and UCE.	542
<i>Mihir Bellare, Igors Stepanovs, and Stefano Tessaro</i>	
Point-Function Obfuscation: A Framework and Generic Constructions.	565
<i>Mihir Bellare and Igors Stepanovs</i>	
Author Index	595