Table of Contents – Part II

Pseudorandom Functions and Applications

Constrained Key-Homomorphic PRFs from Standard Lattice Assumptions (Or: How to Secretly Embed a Circuit in Your PRF) 1
Zvika Brakerski and Vinod Vaikuntanathan

Key-Homomorphic Constrained Pseudorandom Functions 31
Abhishek Banerjee, Georg Fuchsbauer, Chris Peikert, Krzysztof Pietrzak, and Sophie Stevens

Aggregate Pseudorandom Functions and Connections to Learning 61
Aloni Cohen, Shafi Goldwasser, and Vinod Vaikuntanathan

Oblivious Polynomial Evaluation and Secure Set-Intersection from Algebraic PRFs 90
Carmit Hazay

Verifiable Random Functions from Weaker Assumptions 121
Tibor Jager

Proofs and Verifiable Computation

Multi-Client Verifiable Computation with Stronger Security Guarantees 144
S. Dov Gordon, Jonathan Katz, Feng-Hao Liu, Elaine Shi, and Hong-Sheng Zhou

Public Verification of Private Effort 169
Giulia Alberini, Tal Moran, and Alon Rosen

Primary-Secondary-Resolver Membership Proof Systems 199
Moni Naor and Asaf Ziv

Tight Parallel Repetition Theorems for Public-Coin Arguments Using KL-Divergence 229
Kai-Min Chung and Rafael Pass

Stretching Groth-Sahai: NIZK Proofs of Partial Satisfiability 247
Carla Ràfols

Differential Privacy

Outlier Privacy 277
Edward Lui and Rafael Pass

Functional Encryption

Function-Private Functional Encryption in the Private-Key Setting 306
Zvika Brakerski and Gil Segev

Functional Encryption for Randomized Functionalities 325
Vipul Goyal, Abhishek Jain, Venkata Koppula, and Amit Sahai

Functional Encryption for Randomized Functionalities in the Private-Key Setting from Minimal Assumptions 352
Ilan Komargodski, Gil Segev, and Eylon Yogev

Obfuscation

Separations in Circular Security for Arbitrary Length Key Cycles 378
Venkata Koppula, Kim Ramchen, and Brent Waters

ZAPs and Non-Interactive Witness Indistinguishability from Indistinguishability Obfuscation 401
Nir Bitansky and Omer Paneth

Random-Oracle Uninstantiability from Indistinguishability Obfuscation 428
Christina Brzuska, Pooya Farshim, and Arno Mittelbach

On Obfuscation with Random Oracles 456
Ran Canetti, Yael Tauman Kalai, and Omer Paneth

Obfuscation of Probabilistic Circuits and Applications 468
Ran Canetti, Huijia Lin, Stefano Tessaro, and Vinod Vaikuntanathan

Graph-Induced Multilinear Maps from Lattices 498
Craig Gentry, Sergey Gorbunov, and Shai Halevi

Obfuscating Circuits via Composite-Order Graded Encoding 528
Benny Applebaum and Zvika Brakerski

Adaptively Secure Two-Party Computation from Indistinguishability Obfuscation 557
Ran Canetti, Shafi Goldwasser, and Oxana Poburinnaya

Adaptively Secure, Universally Composable, Multiparty Computation in Constant Rounds 586
Dana Dachman-Soled, Jonathan Katz, and Vanishree Rao

Two-Round Adaptively Secure MPC from Indistinguishability Obfuscation 614
Sanjam Garg and Antigoni Polychroniadou

Obfuscation-Based Non-black-box Simulation
and Four Message Concurrent Zero Knowledge for NP 638
Omkant Pandey, Manoj Prabhakaran, and Amit Sahai

Public-Coin Differing-Inputs Obfuscation and Its Applications 668
Yuval Ishai, Omkant Pandey, and Amit Sahai

Author Index 699