

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
<i>Dennis Hofheinz</i>	
Standard Security Does Imply Security Against Selective Opening for Markov Distributions.	282
<i>Georg Fuchsbauer, Felix Heuer, Eike Kiltz, and Krzysztof Pietrzak</i>	
Non-Malleable Encryption: Simpler, Shorter, Stronger	306
<i>Sandro Coretti, Yevgeniy Dodis, Björn Tackmann, and Daniele Venturi</i>	
Verifiable Random Functions from Standard Assumptions	336
<i>Dennis Hofheinz and Tibor Jager</i>	

Complexity of Cryptographic Primitives

Homomorphic Evaluation Requires Depth	365
<i>Andrej Bogdanov and Chin Ho Lee</i>	
On Basing Private Information Retrieval on NP-Hardness	372
<i>Tianren Liu and Vinod Vaikuntanathan</i>	

Obfuscation-Based Cryptographic Constructions

On the Correlation Intractability of Obfuscated Pseudorandom Functions	389
<i>Ran Canetti, Yilei Chen, and Leonid Reyzin</i>	
Reconfigurable Cryptography: A Flexible Approach to Long-Term Security . . .	416
<i>Julia Hesse, Dennis Hofheinz, and Andy Rupp</i>	
Multilinear Maps from Obfuscation	446
<i>Martin R. Albrecht, Pooya Farshim, Dennis Hofheinz, Enrique Larraia, and Kenneth G. Paterson</i>	
Perfect Structure on the Edge of Chaos: Trapdoor Permutations from Indistinguishability Obfuscation	474
<i>Nir Bitansky, Omer Paneth, and Daniel Wichs</i>	

Cryptographic Assumptions (Invited Talk followed by Panel)

Cryptographic Assumptions: A Position Paper	505
<i>Shafi Goldwasser and Yael Tauman Kalai</i>	

Multiparty Computation

Adaptive Security with Quasi-Optimal Rate	525
<i>Brett Hemenway, Rafail Ostrovsky, Silas Richelson, and Alon Rosen</i>	
On the Complexity of Additively Homomorphic UC Commitments.	542
<i>Tore Kasper Frederiksen, Thomas P. Jakobsen, Jesper Buus Nielsen, and Roberto Trifiletti</i>	
Simplified Universal Composability Framework	566
<i>Douglas Wikström</i>	
Characterization of Secure Multiparty Computation Without Broadcast	596
<i>Ran Cohen, Iftach Haitner, Eran Omri, and Lior Rotem</i>	
Author Index	617