

Contents – Part II

Delegation and IP

Delegating RAM Computations with Adaptive Soundness and Privacy	3
<i>Prabhanjan Ananth, Yu-Chi Chen, Kai-Min Chung, Huijia Lin, and Wei-Kai Lin</i>	
Interactive Oracle Proofs	31
<i>Eli Ben-Sasson, Alessandro Chiesa, and Nicholas Spooner</i>	
Adaptive Succinct Garbled RAM or: How to Delegate Your Database.	61
<i>Ran Canetti, Yilei Chen, Justin Holmgren, and Mariana Raykova</i>	
Delegating RAM Computations	91
<i>Yael Kalai and Omer Paneth</i>	

Public-Key Encryption

Standard Security Does Not Imply Indistinguishability Under Selective Opening.	121
<i>Dennis Hofheinz, Vanishree Rao, and Daniel Wichs</i>	
Public-Key Encryption with Simulation-Based Selective-Opening Security and Compact Ciphertexts	146
<i>Dennis Hofheinz, Tibor Jager, and Andy Rupp</i>	
Towards Non-Black-Box Separations of Public Key Encryption and One Way Function.	169
<i>Dana Dachman-Soled</i>	
Post-Quantum Security of the Fujisaki-Okamoto and OAEP Transforms	192
<i>Ehsan Ebrahimi Targhi and Dominique Unruh</i>	
Multi-key FHE from LWE, Revisited	217
<i>Chris Peikert and Sina Shiehian</i>	

Obfuscation and Multilinear Maps

Secure Obfuscation in a Weak Multilinear Map Model	241
<i>Sanjam Garg, Eric Miles, Pratyay Mukherjee, Amit Sahai, Akshayaram Srinivasan, and Mark Zhandry</i>	

Virtual Grey-Boxes Beyond Obfuscation: A Statistical Security Notion for Cryptographic Agents	269
<i>Shashank Agrawal, Manoj Prabhakaran, and Ching-Hua Yu</i>	

Attribute-Based Encryption

Deniable Attribute Based Encryption for Branching Programs from LWE . . .	299
<i>Daniel Apon, Xiong Fan, and Feng-Hao Liu</i>	
Targeted Homomorphic Attribute-Based Encryption	330
<i>Zvika Brakerski, David Cash, Rotem Tsabary, and Hoeteck Wee</i>	
Semi-adaptive Security and Bundling Functionalities Made Generic and Easy	361
<i>Rishab Goyal, Venkata Koppula, and Brent Waters</i>	

Functional Encryption

From Cryptomania to Obfustopia Through Secret-Key Functional Encryption	391
<i>Nir Bitansky, Ryo Nishimaki, Alain Passelègue, and Daniel Wichs</i>	
Single-Key to Multi-Key Functional Encryption with Polynomial Loss	419
<i>Sanjam Garg and Akshayaram Srinivasan</i>	
Compactness vs Collusion Resistance in Functional Encryption	443
<i>Baiyu Li and Daniele Micciancio</i>	

Secret Sharing

Threshold Secret Sharing Requires a Linear Size Alphabet.	471
<i>Andrej Bogdanov, Siyao Guo, and Ilan Komargodski</i>	
How to Share a Secret, Infinitely	485
<i>Ilan Komargodski, Moni Naor, and Eylon Yogev</i>	

New Models

Designing Proof of Human-Work Puzzles for Cryptocurrency and Beyond. . .	517
<i>Jeremiah Blocki and Hong-Sheng Zhou</i>	
Access Control Encryption: Enforcing Information Flow with Cryptography	547
<i>Ivan Damgård, Helene Haagh, and Claudio Orlandi</i>	

Author Index	577
-------------------------------	-----