

Table of Contents

Hardness Amplification

Input Locality and Hardness Amplification	1
<i>Andrej Bogdanov and Alon Rosen</i>	
General Hardness Amplification of Predicates and Puzzles	19
<i>Thomas Holenstein and Grant Schoenebeck</i>	
Security Amplification for the Cascade of Arbitrarily Weak PRPs: Tight Bounds via the Interactive Hardcore Lemma	37
<i>Stefano Tessaro</i>	

Invited Talk 1

Dense Model Theorems and Their Applications	55
<i>Luca Trevisan</i>	

Leakage Resilience

Parallel Repetition for Leakage Resilience Amplification Revisited	58
<i>Abhishek Jain and Krzysztof Pietrzak</i>	
Achieving Leakage Resilience through Dual System Encryption	70
<i>Allison Lewko, Yannis Rouselakis, and Brent Waters</i>	
Signatures Resilient to Continual Leakage on Memory and Computation	89
<i>Tal Malkin, Isamu Teranishi, Yevgeniy Vahlis, and Moti Yung</i>	
After-the-Fact Leakage in Public-Key Encryption	107
<i>Shai Halevi and Huijia Lin</i>	

Tamper Resilience

One-Time Computable Self-erasing Functions	125
<i>Stefan Dziembowski, Tomasz Kazana, and Daniel Wichs</i>	
Perfectly Secure Oblivious RAM without Random Oracles	144
<i>Ivan Damgård, Sigurd Meldgaard, and Jesper Buus Nielsen</i>	
Unconditional and Composable Security Using a Single Stateful Tamper-Proof Hardware Token	164
<i>Nico Döttling, Daniel Kraschewski, and Jörn Müller-Quade</i>	

Correlated-Input Secure Hash Functions	182
<i>Vipul Goyal, Adam O'Neill, and Vanishree Rao</i>	

Encryption

Black-Box Circular-Secure Encryption beyond Affine Functions	201
<i>Zvika Brakerski, Shafi Goldwasser, and Yael Tauman Kalai</i>	
Homomorphic Encryption: From Private-Key to Public-Key	219
<i>Ron Rothblum</i>	
Identity-Based Encryption Secure against Selective Opening Attack	235
<i>Mihir Bellare, Brent Waters, and Scott Yilek</i>	
Functional Encryption: Definitions and Challenges	253
<i>Dan Boneh, Amit Sahai, and Brent Waters</i>	

Composable Security

Concurrent Non-Malleable Zero Knowledge with Adaptive Inputs	274
<i>Huijia Lin and Rafael Pass</i>	
Round-Optimal Password-Based Authenticated Key Exchange	293
<i>Jonathan Katz and Vinod Vaikuntanathan</i>	
Bringing People of Different Beliefs Together to Do UC	311
<i>Sanjam Garg, Vipul Goyal, Abhishek Jain, and Amit Sahai</i>	

Secure Computation

Secure Two-Party Computation via Cut-and-Choose Oblivious Transfer	329
<i>Yehuda Lindell and Benny Pinkas</i>	
Practical Adaptive Oblivious Transfer from Simple Assumptions	347
<i>Matthew Green and Susan Hohenberger</i>	
Completeness Theorems with Constructive Proofs for Finite Deterministic 2-Party Functions	364
<i>Daniel Kraschewski and Jörn Müller-Quade</i>	
A Zero-One Law for Secure Multi-party Computation with Ternary Outputs	382
<i>Gunnar Kreitz</i>	

Privacy

PCPs and the Hardness of Generating Private Synthetic Data	400
<i>Jonathan Ullman and Salil Vadhan</i>	
Limits of Computational Differential Privacy in the Client/Server Setting	417
<i>Adam Groce, Jonathan Katz, and Arkady Yerukhimovich</i>	
Towards Privacy for Social Networks: A Zero-Knowledge Based Definition of Privacy	432
<i>Johannes Gehrke, Edward Lui, and Rafael Pass</i>	

Coin Tossing and Pseudorandomness

On the Black-Box Complexity of Optimally-Fair Coin Tossing	450
<i>Dana Dachman-Soled, Yehuda Lindell, Mohammad Mahmoody, and Tal Malkin</i>	
Tight Bounds for Classical and Quantum Coin Flipping	468
<i>Esther Hänggi and Jürg Wullschlegel</i>	
Exploring the Limits of Common Coins Using Frontier Analysis of Protocols	486
<i>Hemanta K. Maji, Pichayoot Ouppaphan, Manoj Prabhakaran, and Mike Rosulek</i>	
Limits on the Stretch of Non-adaptive Constructions of Pseudo-Random Generators	504
<i>Josh Bronson, Ali Juma, and Periklis A. Papakonstantinou</i>	
On the Complexity of Non-adaptively Increasing the Stretch of Pseudorandom Generators	522
<i>Eric Miles and Emanuele Viola</i>	

Invited Talk 2

Concurrent Security and Non-malleability (Abstract)	540
<i>Rafael Pass</i>	

Black-Box Constructions and Separations

(Nearly) Round-Optimal Black-Box Constructions of Commitments Secure against Selective Opening Attacks	541
<i>David Xiao</i>	

Limits on the Power of Zero-Knowledge Proofs in Cryptographic Constructions	559
<i>Zvika Brakerski, Jonathan Katz, Gil Segev, and Arkady Yerukhimovich</i>	
Towards Non-black-Box Lower Bounds in Cryptography	579
<i>Rafael Pass, Wei-Lung Dustin Tseng, and Muthuramakrishnan Venkitasubramaniam</i>	
Black-Box Separations	
On Black-Box Separations among Injective One-Way Functions	597
<i>Takahiro Matsuda and Kanta Matsuura</i>	
Impossibility of Blind Signatures from One-Way Permutations	615
<i>Jonathan Katz, Dominique Schröder, and Arkady Yerukhimovich</i>	
Author Index	631