

Table of Contents

Overcoming Weak Expectations.....	1
<i>Yevgeniy Dodis and Yu Yu</i>	
A Counterexample to the Chain Rule for Conditional HILL Entropy: And What Deniable Encryption Has to Do with It	23
<i>Stephan Krenn, Krzysztof Pietrzak, and Akshay Wadia</i>	
Hardness Preserving Reductions via Cuckoo Hashing	40
<i>Itay Berman, Iftach Haitner, Ilan Komargodski, and Moni Naor</i>	
Concurrent Zero Knowledge in the Bounded Player Model	60
<i>Vipul Goyal, Abhishek Jain, Rafail Ostrovsky, Silas Richelson, and Ivan Visconti</i>	
Public-Coin Concurrent Zero-Knowledge in the Global Hash Model	80
<i>Ran Canetti, Huijia Lin, and Omer Paneth</i>	
Succinct Malleable NIZKs and an Application to Compact Shuffles	100
<i>Melissa Chase, Markulf Kohlweiss, Anna Lysyanskaya, and Sarah Meiklejohn</i>	
Encrypted Messages from the Heights of Cryptomania	120
<i>Craig Gentry</i>	
Attribute-Based Functional Encryption on Lattices	122
<i>Xavier Boyen</i>	
When Homomorphism Becomes a Liability	143
<i>Zvika Brakerski</i>	
Garbling XOR Gates “For Free” in the Standard Model	162
<i>Benny Applebaum</i>	
Why “Fiat-Shamir for Proofs” Lacks a Proof	182
<i>Nir Bitansky, Dana Dachman-Soled, Sanjam Garg, Abhishek Jain, Yael Tauman Kalai, Adriana López-Alt, and Daniel Wichs</i>	
On the (In)security of Fischlin’s Paradigm	202
<i>Prabhanjan Ananth, Raghav Bhaskar, Vipul Goyal, and Vanishree Rao</i>	
Signatures of Correct Computation	222
<i>Charalampos Papamanthou, Elaine Shi, and Roberto Tamassia</i>	

A Full Characterization of Functions that Imply Fair Coin Tossing and Ramifications to Fairness.....	243
<i>Gilad Asharov, Yehuda Lindell, and Tal Rabin</i>	
Characterizing the Cryptographic Properties of Reactive 2-Party Functionalities.....	263
<i>R. Amzi Jeffs and Mike Rosulek</i>	
Feasibility and Completeness of Cryptographic Tasks in the Quantum World.....	281
<i>Serge Fehr, Jonathan Katz, Fang Song, Hong-Sheng Zhou, and Vassilis Zikas</i>	
Languages with Efficient Zero-Knowledge PCPs are in SZK.....	297
<i>Mohammad Mahmoody and David Xiao</i>	
Succinct Non-interactive Arguments via Linear Interactive Proofs.....	315
<i>Nir Bitansky, Alessandro Chiesa, Yuval Ishai, Omer Paneth, and Rafail Ostrovsky</i>	
Unprovable Security of Perfect NIZK and Non-interactive Non-malleable Commitments.....	334
<i>Rafael Pass</i>	
Secure Computation for Big Data.....	355
<i>Tal Malkin</i>	
Communication Locality in Secure Multi-party Computation: How to Run Sublinear Algorithms in a Distributed Setting.....	356
<i>Elette Boyle, Shafi Goldwasser, and Stefano Tessaro</i>	
Distributed Oblivious RAM for Secure Two-Party Computation.....	377
<i>Steve Lu and Rafail Ostrovsky</i>	
Black-Box Proof of Knowledge of Plaintext and Multiparty Computation with Low Communication Overhead.....	397
<i>Steven Myers, Mona Sergi, and abhi shelat</i>	
Testing the Lipschitz Property over Product Distributions with Applications to Data Privacy.....	418
<i>Kashyap Dixit, Madhav Jha, Sofya Raskhodnikova, and Abhradeep Thakurta</i>	
Limits on the Usefulness of Random Oracles.....	437
<i>Iftach Haitner, Eran Omri, and Hila Zarosim</i>	
Analyzing Graphs with Node Differential Privacy.....	457
<i>Shiva Prasad Kasiviswanathan, Kobbi Nissim, Sofya Raskhodnikova, and Adam Smith</i>	

Universally Composable Synchronous Computation	477
<i>Jonathan Katz, Ueli Maurer, Björn Tackmann, and Vassilis Zikas</i>	
Multi-Client Non-interactive Verifiable Computation	499
<i>Seung Geol Choi, Jonathan Katz, Ranjit Kumaresan, and Carlos Cid</i>	
On the Feasibility of Extending Oblivious Transfer	519
<i>Yehuda Lindell and Hila Zarosim</i>	
Computational Soundness of Coinductive Symbolic Security under Active Attacks	539
<i>Mohammad Hajiabadi and Bruce M. Kapron</i>	
Revisiting Lower and Upper Bounds for Selective Decommitments	559
<i>Rafail Ostrovsky, Vanishree Rao, Alessandra Scafuro, and Ivan Visconti</i>	
On the Circular Security of Bit-Encryption	579
<i>Ron D. Rothblum</i>	
Cryptographic Hardness of Random Local Functions – Survey	599
<i>Benny Applebaum</i>	
On the Power of Correlated Randomness in Secure Computation	600
<i>Yuval Ishai, Eyal Kushilevitz, Sigurd Meldgaard, Claudio Orlandi, and Anat Paskin-Cherniavsky</i>	
Constant-Overhead Secure Computation of Boolean Circuits using Preprocessing	621
<i>Ivan Damgård and Sarah Zakarias</i>	
Implementing Resettable UC-Functionalities with Untrusted Tamper-Proof Hardware-Tokens	642
<i>Nico Döttling, Thilo Mie, Jörn Müller-Quade, and Tobias Nilges</i>	
A Cookbook for Black-Box Separations and a Recipe for UOWHFs	662
<i>Kfir Barhum and Thomas Holenstein</i>	
Algebraic (Trapdoor) One-Way Functions and Their Applications	680
<i>Dario Catalano, Dario Fiore, Rosario Gennaro, and Konstantinos Vamvourellis</i>	
Randomness-Dependent Message Security	700
<i>Eleanor Birrell, Kai-Min Chung, Rafael Pass, and Sidharth Telang</i>	
Errata to <i>(Nearly) Round-Optimal Black-Box Constructions of Commitments Secure against Selective Opening Attacks</i>	721
<i>David Xiao</i>	
Author Index	723