

Table of Contents

Obfuscation

Virtual Black-Box Obfuscation for All Circuits via Generic Graded Encoding	1
<i>Zvika Brakerski and Guy N. Rothblum</i>	
Obfuscation for Evasive Functions	26
<i>Boaz Barak, Nir Bitansky, Ran Canetti, Yael Tauman Kalai, Omer Paneth, and Amit Sahai</i>	
On Extractability Obfuscation	52
<i>Elette Boyle, Kai-Min Chung, and Rafael Pass</i>	

Applications of Obfuscation

Two-Round Secure MPC from Indistinguishability Obfuscation	74
<i>Sanjam Garg, Craig Gentry, Shai Halevi, and Mariana Raykova</i>	
Chosen Ciphertext Security via Point Obfuscation	95
<i>Takahiro Matsuda and Goichiro Hanaoka</i>	

Zero Knowledge

Probabilistically Checkable Proofs of Proximity with Zero-Knowledge ...	121
<i>Yuval Ishai and Mor Weiss</i>	
Achieving Constant Round Leakage-Resilient Zero-Knowledge	146
<i>Omkant Pandey</i>	
Statistical Concurrent Non-malleable Zero Knowledge	167
<i>Claudio Orlandi, Rafail Ostrovsky, Vanishree Rao, Amit Sahai, and Ivan Visconti</i>	
4-Round Resetably-Sound Zero Knowledge	192
<i>Kai-Min Chung, Rafail Ostrovsky, Rafael Pass, Muthuramakrishnan Venkitasubramaniam, and Ivan Visconti</i>	

Black-Box Separations

Can Optimally-Fair Coin Tossing Be Based on One-Way Functions?	217
<i>Dana Dachman-Soled, Mohammad Mahmoody, and Tal Malkin</i>	

On the Power of Public-Key Encryption in Secure Computation	240
<i>Mohammad Mahmoody, Hemanta K. Maji, and Manoj Prabhakaran</i>	
On the Impossibility of Basing Public-Coin One-Way Permutations on Trapdoor Permutations	265
<i>Takahiro Matsuda</i>	

Secure Computation

Towards Characterizing Complete Fairness in Secure Two-Party Computation	291
<i>Gilad Asharov</i>	
On the Cryptographic Complexity of the Worst Functions	317
<i>Amos Beimel, Yuval Ishai, Ranjit Kumaresan, and Eyal Kushilevitz</i>	
Constant-Round Black-Box Construction of Composable Multi-Party Computation Protocol	343
<i>Susumu Kiyoshima, Yoshifumi Manabe, and Tatsuaki Okamoto</i>	
One-Sided Adaptively Secure Two-Party Computation	368
<i>Carmit Hazay and Arpita Patra</i>	
Multi-linear Secret-Sharing Schemes	394
<i>Amos Beimel, Aner Ben-Efraim, Carles Padró, and Ilya Tyomkin</i>	
Broadcast Amplification	419
<i>Martin Hirt, Ueli Maurer, and Pavel Raykov</i>	

Coding and Cryptographic Applications

Non-malleable Coding against Bit-Wise and Split-State Tampering	440
<i>Mahdi Cheraghchi and Venkatesan Guruswami</i>	
Continuous Non-malleable Codes	465
<i>Sebastian Faust, Pratyay Mukherjee, Jesper Buus Nielsen, and Daniele Venturi</i>	
Locally Updatable and Locally Decodable Codes	489
<i>Nishanth Chandran, Bhavana Kanukurthi, and Rafail Ostrovsky</i>	

Leakage

Leakage Resilient Fully Homomorphic Encryption	515
<i>Alexandra Berkoff and Feng-Hao Liu</i>	
Securing Circuits and Protocols against $1/\text{poly}(k)$ Tampering Rate	540
<i>Dana Dachman-Soled and Yael Tauman Kalai</i>	

How to Fake Auxiliary Input	566
<i>Dimitar Jetchev and Krzysztof Pietrzak</i>	

Encryption

Standard versus Selective Opening Security: Separation and Equivalence Results	591
<i>Dennis Hofheinz and Andy Rupp</i>	

Dual System Encryption via Predicate Encodings	616
<i>Hoeteck Wee</i>	

Hardware-Aided Secure Protocols

(Efficient) Universally Composable Oblivious Transfer Using a Minimal Number of Stateless Tokens	638
<i>Seung Geol Choi, Jonathan Katz, Dominique Schröder, Arkady Yerukhimovich, and Hong-Sheng Zhou</i>	

Lower Bounds in the Hardware Token Model	663
<i>Shashank Agrawal, Prabhanjan Ananth, Vipul Goyal, Manoj Prabhakaran, and Alon Rosen</i>	

Encryption and Signatures

Unified, Minimal and Selectively Randomizable Structure-Preserving Signatures	688
<i>Masayuki Abe, Jens Groth, Miyako Ohkubo, and Mehdi Tibouchi</i>	

On the Impossibility of Structure-Preserving Deterministic Primitives	713
<i>Masayuki Abe, Jan Camenisch, Rafael Dowsley, and Maria Dubovitskaya</i>	

Author Index	739
--------------------	-----