

Table of Contents – Part I

Foundations

On Basing Size-Verifiable One-Way Functions on NP-Hardness	1
<i>Andrej Bogdanov and Christina Brzuska</i>	
The Randomized Iterate, Revisited - Almost Linear Seed Length PRGs from a Broader Class of One-Way Functions	7
<i>Yu Yu, Dawu Gu, Xiangxue Li, and Jian Weng</i>	
The Power of Negations in Cryptography	36
<i>Siyao Guo, Tal Malkin, Igor C. Oliveira, and Alon Rosen</i>	
From Weak to Strong Zero-Knowledge and Applications	66
<i>Kai-Min Chung, Edward Lui, and Rafael Pass</i>	
An Efficient Transform from Sigma Protocols to NIZK with a CRS and Non-programmable Random Oracle	93
<i>Yehuda Lindell</i>	

Symmetric Key

On the Indifferentiability of Key-Alternating Feistel Ciphers with No Key Derivation	110
<i>Chun Guo and Dongdai Lin</i>	

Multiparty Computation

A Little Honesty Goes a Long Way: The Two-Tier Model for Secure Multiparty Computation	134
<i>Juan A. Garay, Ran Gelles, David S. Johnson, Aggelos Kiayias, and Moti Yung</i>	
Topology-Hiding Computation	159
<i>Tal Moran, Ilan Orlov, and Silas Richelson</i>	
Secure Physical Computation Using Disposable Circuits	182
<i>Ben A. Fisch, Daniel Freund, and Moni Naor</i>	
Complete Characterization of Fairness in Secure Two-Party Computation of Boolean Functions	199
<i>Gilad Asharov, Amos Beimel, Nikolaos Makriyannis, and Eran Omri</i>	

Richer Efficiency/Security Trade-offs in 2PC	229
<i>Vladimir Kolesnikov, Payman Mohassel, Ben Riva, and Mike Rosulek</i>	

Concurrent and Resettable Security

Round-Efficient Concurrently Composable Secure Computation via a Robust Extraction Lemma	260
<i>Vipul Goyal, Huijia Lin, Omkant Pandey, Rafael Pass, and Amit Sahai</i>	
An Alternative Approach to Non-black-box Simulation in Fully Concurrent Setting	290
<i>Susumu Kiyoshima</i>	
General Statistically Secure Computation with Bounded-Resettable Hardware Tokens	319
<i>Nico Döttling, Daniel Kraschewski, Jörn Müller-Quade, and Tobias Nilges</i>	
Resetably Sound Zero-Knowledge Arguments from OWFs - The (Semi) Black-Box Way	345
<i>Rafail Ostrovsky, Alessandra Scafuro, and Muthuramakrishnan Venkitasubramanian</i>	

Non-malleable Codes and Tampering

A Rate-Optimizing Compiler for Non-malleable Codes Against Bit-Wise Tampering and Permutations	375
<i>Shashank Agrawal, Divya Gupta, Hemanta K. Maji, Omkant Pandey, and Manoj Prabhakaran</i>	
Leakage-Resilient Non-malleable Codes	398
<i>Divesh Aggarwal, Stefan Dziembowski, Tomasz Kazana, and Maciej Obremski</i>	
Locally Decodable and Updatable Non-malleable Codes and Their Applications	427
<i>Dana Dachman-Soled, Feng-Hao Liu, Elaine Shi, and Hong-Sheng Zhou</i>	
Tamper Detection and Continuous Non-malleable Codes	451
<i>Zahra Jafargholi and Daniel Wichs</i>	
Optimal Algebraic Manipulation Detection Codes in the Constant-Error Model	481
<i>Ronald Cramer, Carles Padró, and Chaoping Xing</i>	

Privacy Amplification

Non-malleable Condensers for Arbitrary Min-entropy, and Almost Optimal Protocols for Privacy Amplification	502
<i>Xin Li</i>	

Encryption and Key Exchange

From Single-Bit to Multi-bit Public-Key Encryption via Non-malleable Codes	532
<i>Sandro Coretti, Ueli Maurer, Björn Tackmann, and Daniele Venturi</i>	

Constructing and Understanding Chosen Ciphertext Security via Puncturable Key Encapsulation Mechanisms	561
<i>Takahiro Matsuda and Goichiro Hanaoka</i>	

Non-committing Encryption from Φ -hiding	591
<i>Brett Hemenway, Rafail Ostrovsky, and Alon Rosen</i>	

On the Regularity of Lossy RSA: Improved Bounds and Applications to Padding-Based Encryption	609
<i>Adam Smith and Ye Zhang</i>	

Tightly-Secure Authenticated Key Exchange	629
<i>Christoph Bader, Dennis Hofheinz, Tibor Jager, Eike Kiltz, and Yong Li</i>	

Author Index	659
------------------------	-----