Contents

Practical Sharing of Quantum Secrets over Untrusted Channels ........ 1
Damian Markham and Anne Marin

Generalizing Efficient Multiparty Computation .................... 15
Bernardo M. David, Ryo Nishimaki, Samuel Ranellucci,
and Alain Tapp

Round-Optimal Perfectly Secret Message Transmission with Linear
Communication Complexity ....................................... 33
Ravi Kishore, Ashutosh Kumar, Chiranjeevi Vanarasa,
and Srinathan Kannan

On Zero-Knowledge with Strict Polynomial-Time Simulation and
Extraction from Differing-Input Obfuscation for Circuits ............ 51
Ning Ding

Unifying Leakage Classes: Simulatable Leakage and Pseudoentropy ...... 69
Benjamin Fuller and Ariel Hamlin

On the Orthogonal Vector Problem and the Feasibility of
Unconditionally Secure Leakage-Resilient Computation ............... 87
Ivan Damgård, Frédéric Dupuis, and Jesper Buus Nielsen

Metric Pseudoentropy: Characterizations, Transformations and
Applications ..................................................... 105
Maciej Skorski

Nonuniform Indistinguishability and Unpredictability Hardcore
Lemmas: New Proofs and Applications to Pseudoentropy .......... 123
Maciej Skorski

Gambling, Computational Information and Encryption Security....... 141
Mohammad Hajiabadi and Bruce M. Kapron

Query-Complexity Amplification for Random Oracles ................. 159
Grégory Demay, Peter Gaži, Ueli Maurer, and Björn Tackmann

The Chaining Lemma and Its Application ........................ 181
Ivan Damgård, Sebastian Faust, Pratyay Mukherjee,
and Daniele Venturi
Weakening the Isolation Assumption of Tamper-Proof Hardware Tokens ...................................................... 197
   Rafael Dowsley, Jörn Müller-Quade, and Tobias Nilges

Limited View Adversary Codes: Bounds, Constructions and Applications .................................................... 214
   Pengwei Wang and Reihaneh Safavi-Naini

Locally Decodable Codes for Edit Distance .............................................. 236
   Rafail Ostrovsky and Anat Paskin-Cherniavsky

The Multivariate Hidden Number Problem ........................................... 250
   Steven D. Galbraith and Barak Shani

Lattice Point Enumeration on Block Reduced Bases ............................... 269
   Michael Walter

Adaptive Key Recovery Attacks on NTRU-Based Somewhat Homomorphic Encryption Schemes ...................... 283
   Ricardo Dahab, Steven D. Galbraith, and Eduardo Morais

Author Index .................................................................................. 297
Information Theoretic Security
8th International Conference, ICITS 2015, Lugano, Switzerland, May 2-5, 2015. Proceedings
Lehmann, A.; Wolf, S. (Eds.)
2015, XIV, 297 p. 29 illus., Softcover
ISBN: 978-3-319-17469-3