

Contents

| | |
|------------------------------------------------------------------------------------------------------------------------------------|-----|
| Practical Sharing of Quantum Secrets over Untrusted Channels | 1 |
| <i>Damian Markham and Anne Marin</i> | |
| Generalizing Efficient Multiparty Computation | 15 |
| <i>Bernardo M. David, Ryo Nishimaki, Samuel Ranellucci, and Alain Tapp</i> | |
| Round-Optimal Perfectly Secret Message Transmission with Linear Communication Complexity | 33 |
| <i>Ravi Kishore, Ashutosh Kumar, Chiranjeevi Vanarasa, and Srinathan Kannan</i> | |
| On Zero-Knowledge with Strict Polynomial-Time Simulation and Extraction from Differing-Input Obfuscation for Circuits | 51 |
| <i>Ning Ding</i> | |
| Unifying Leakage Classes: Simulatable Leakage and Pseudoentropy | 69 |
| <i>Benjamin Fuller and Ariel Hamlin</i> | |
| On the Orthogonal Vector Problem and the Feasibility of Unconditionally Secure Leakage-Resilient Computation | 87 |
| <i>Ivan Damgård, Frédéric Dupuis, and Jesper Buus Nielsen</i> | |
| Metric Pseudoentropy: Characterizations, Transformations and Applications | 105 |
| <i>Maciej Skorski</i> | |
| Nonuniform Indistinguishability and Unpredictability Hardcore Lemmas: New Proofs and Applications to Pseudoentropy | 123 |
| <i>Maciej Skorski</i> | |
| Gambling, Computational Information and Encryption Security | 141 |
| <i>Mohammad Hajiabadi and Bruce M. Kapron</i> | |
| Query-Complexity Amplification for Random Oracles | 159 |
| <i>Grégory Demay, Peter Gaži, Ueli Maurer, and Björn Tackmann</i> | |
| The Chaining Lemma and Its Application | 181 |
| <i>Ivan Damgård, Sebastian Faust, Pratyay Mukherjee, and Daniele Venturi</i> | |

| | |
|----------------------------------------------------------------------------------------------|-----|
| Weakening the Isolation Assumption of Tamper-Proof Hardware Tokens | 197 |
| <i>Rafael Dowsley, Jörn Müller-Quade, and Tobias Nilges</i> | |
| Limited View Adversary Codes: Bounds, Constructions and Applications | 214 |
| <i>Pengwei Wang and Reihaneh Safavi-Naini</i> | |
| Locally Decodable Codes for Edit Distance | 236 |
| <i>Rafail Ostrovsky and Anat Paskin-Cherniavsky</i> | |
| The Multivariate Hidden Number Problem | 250 |
| <i>Steven D. Galbraith and Barak Shani</i> | |
| Lattice Point Enumeration on Block Reduced Bases | 269 |
| <i>Michael Walter</i> | |
| Adaptive Key Recovery Attacks on NTRU-Based Somewhat Homomorphic Encryption Schemes | 283 |
| <i>Ricardo Dahab, Steven D. Galbraith, and Eduardo Morais</i> | |
| 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