

# Contents

## Secret Sharing

Efficient Threshold Secret Sharing Schemes Secure Against Rushing Cheaters . . . . .	3
<i>Avishek Adhikari, Kirill Morozov, Satoshi Obana, Partha Sarathi Roy, Kouichi Sakurai, and Rui Xu</i>	
Dynamic and Verifiable Hierarchical Secret Sharing . . . . .	24
<i>Giulia Traverso, Denise Demirel, and Johannes Buchmann</i>	

## Quantum Cryptography

Computational Security of Quantum Encryption . . . . .	47
<i>Gorjan Alagic, Anne Broadbent, Bill Fefferman, Tommaso Gagliardoni, Christian Schaffner, and Michael St. Jules</i>	
Efficient Simulation for Quantum Message Authentication . . . . .	72
<i>Anne Broadbent and Evelyn Wainewright</i>	

## Visual Cryptography

Private Visual Share-Homomorphic Computation and Randomness Reduction in Visual Cryptography. . . . .	95
<i>Paolo D'Arco, Roberto De Prisco, and Yvo Desmedt</i>	
Revisiting the False Acceptance Rate Attack on Biometric Visual Cryptographic Schemes . . . . .	114
<i>Koray Karabina and Angela Robinson</i>	

## Cryptographic Protocols

Detecting Algebraic Manipulation in Leaky Storage Systems . . . . .	129
<i>Fuchun Lin, Reihaneh Safavi-Naini, and Pengwei Wang</i>	
Cheater Detection in SPDZ Multiparty Computation . . . . .	151
<i>Gabriele Spini and Serge Fehr</i>	
Error-Correcting Codes Against Chosen-Codeword Attacks . . . . .	177
<i>Kenji Yasunaga</i>	

Efficient Generic Zero-Knowledge Proofs from Commitments (Extended Abstract). . . . .	190
<i>Samuel Ranellucci, Alain Tapp, and Rasmus Zakarias</i>	
Unconditionally Secure Revocable Storage: Tight Bounds, Optimal Construction, and Robustness . . . . .	213
<i>Yohei Watanabe, Goichiro Hanaoka, and Junji Shikata</i>	
<b>Entropy, Extractors and Privacy</b>	
A Practical Fuzzy Extractor for Continuous Features . . . . .	241
<i>Vladimir P. Parente and Jeroen van de Graaf</i>	
Almost Perfect Privacy for Additive Gaussian Privacy Filters . . . . .	259
<i>Shahab Asoodeh, Fady Alajaji, and Tamás Linder</i>	
A Better Chain Rule for HILL Pseudoentropy - Beyond Bounded Leakage . . . .	279
<i>Maciej Skórski</i>	
<b>Author Index</b> . . . . .	301

Information Theoretic Security

9th International Conference, ICITS 2016, Tacoma, WA,  
USA, August 9-12, 2016, Revised Selected Papers

Nascimento, A.C.A.; Barreto, P. (Eds.)

2016, VIII, 301 p. 28 illus., Softcover

ISBN: 978-3-319-49174-5