

# Contents

How to Construct Strongly Secure Network Coding Scheme . . . . .	1
<i>Kaoru Kurosawa, Hiroyuki Ohta, and Kenji Kakuta</i>	
Secure Two-Party Computation: A Visual Way . . . . .	18
<i>Paolo D'Arco and Roberto De Prisco</i>	
Measure-Independent Characterization of Contrast Optimal Visual Cryptography Schemes . . . . .	39
<i>Paolo D'Arco, Roberto De Prisco, and Alfredo De Santis</i>	
On $(k, n)$ Visual Cryptography Scheme with $t$ Essential Parties . . . . .	56
<i>Teng Guo, Feng Liu, ChuanKun Wu, YaWei Ren, and Wen Wang</i>	
New Lower Bounds for Privacy in Communication Protocols . . . . .	69
<i>Iordanis Kerenidis, Mathieu Laurière, and David Xiao</i>	
On the Transmit Beamforming for MIMO Wiretap Channels: Large-System Analysis . . . . .	90
<i>Maksym A. Girnyk, Frédéric Gabry, Mikko Vehkaperä, Lars K. Rasmussen, and Mikael Skoglund</i>	
Information Theoretic Security for Encryption Based on Conditional Rényi Entropies . . . . .	103
<i>Mitsugu Iwamoto and Junji Shikata</i>	
Insider-Proof Encryption with Applications for Quantum Key Distribution . . .	122
<i>Matthew McKague and Lana Sheridan</i>	
Superposition Attacks on Cryptographic Protocols . . . . .	142
<i>Ivan Damgård, Jakob Funder, Jesper Buus Nielsen, and Louis Salvail</i>	
Overcoming Weak Expectations via the Rényi Entropy and the Expanded Computational Entropy . . . . .	162
<i>Yanqing Yao and Zhoujun Li</i>	
Modulus Computational Entropy . . . . .	179
<i>Maciej Skórski</i>	
Broadcast (and Round) Efficient Verifiable Secret Sharing . . . . .	200
<i>Juan Garay, Clint Givens, Rafail Ostrovsky, and Pavel Raykov</i>	
Leakage Resilience of the Blom's Key Distribution Scheme . . . . .	220
<i>Michał Jastrzębski and Stefan Dziembowski</i>	

Detection of Algebraic Manipulation in the Presence of Leakage . . . . . 238  
    *Hadi Ahmadi and Reihaneh Safavi-Naini*

**Author Index** . . . . . 259

Information Theoretic Security

7th International Conference, ICITS 2013, Singapore,

November 28-30, 2013, Proceedings

Padró, C. (Ed.)

2014, XII, 259 p. 29 illus., Softcover

ISBN: 978-3-319-04267-1