

Contents

Linear-Time Non-Malleable Codes in the Bit-Wise Independent Tampering Model	1
<i>Ronald Cramer, Ivan Damgård, Nico Döttling, Irene Giacomelli, and Chaoping Xing</i>	
Disproving the Conjectures from “On the Complexity of Scrypt and Proofs of Space in the Parallel Random Oracle Model”	26
<i>Daniel Malinowski and Karol Żebrowski</i>	
Broadcast Encryption with Guessing Secrecy	39
<i>Yohei Watanabe</i>	
Contrast Optimal XOR Based Visual Cryptographic Schemes.	58
<i>Sabyasachi Dutta and Avishek Adhikari</i>	
Verifiably Multiplicative Secret Sharing	73
<i>Maki Yoshida and Satoshi Obana</i>	
Round and Communication Efficient Unconditionally-Secure MPC with $t < n/3$ in Partially Synchronous Network	83
<i>Ashish Choudhury, Arpita Patra, and Divya Ravi</i>	
Catching MPC Cheaters: Identification and Openability	110
<i>Robert Cunningham, Benjamin Fuller, and Sophia Yakubov</i>	
Secure Grouping Protocol Using a Deck of Cards	135
<i>Yuji Hashimoto, Kazumasa Shinagawa, Koji Nuida, Masaki Inamura, and Goichiro Hanaoka</i>	
Four Cards Are Sufficient for a Card-Based Three-Input Voting Protocol Utilizing Private Permutations.	153
<i>Takeshi Nakai, Satoshi Shirouchi, Mitsugu Iwamoto, and Kazuo Ohta</i>	
Single-Shot Secure Quantum Network Coding for General Multiple Unicast Network with Free Public Communication	166
<i>Go Kato, Masaki Owari, and Masahito Hayashi</i>	

Secure Network Coding for Multiple Unicast: On the Case of Single Source	188
<i>Gaurav Kumar Agarwal, Martina Cardone, and Christina Fragouli</i>	
Rényi Resolvability and Its Applications to the Wiretap Channel	208
<i>Lei Yu and Vincent Y. F. Tan</i>	
Author Index	235

Information Theoretic Security

10th International Conference, ICITS 2017, Hong Kong,
China, November 29 – December 2, 2017, Proceedings

Shikata, J. (Ed.)

2017, XII, 235 p. 31 illus., Softcover

ISBN: 978-3-319-72088-3