

Contents

Faster Zero-Knowledge Protocols and Applications (Invited Talk Abstract).	1
<i>Claudio Orlandi</i>	
Stochastic Side-Channel Leakage Analysis <i>via</i> Orthonormal Decomposition . . .	12
<i>Sylvain Guilley, Annelie Heuser, Tang Ming, and Olivier Rioul</i>	
Key-Policy Attribute-Based Encryption from Bilinear Maps	28
<i>Ferucio Laurențiu Țiplea, Constantin Cătălin Drăgan, and Anca-Maria Nica</i>	
Security of Pseudo-Random Number Generators with Input (Invited Talk)	43
<i>Damien Vergnaud</i>	
Securing the Foundations of Democracy	52
<i>Peter Y.A. Ryan</i>	
Exploring Naccache-Stern Knapsack Encryption	67
<i>Éric Brier, Rémi Géraud, and David Naccache</i>	
Proximity Assurances Based on Natural and Artificial Ambient Environments	83
<i>Iakovos Gurulian, Konstantinos Markantonakis, Carlton Shepherd, Eibe Frank, and Raja Naeem Akram</i>	
Challenges of Federating National Data Access Infrastructures	104
<i>Margus Freudenthal and Jan Willemsen</i>	
Strongly Deniable Identification Schemes Immune to Prover's and Verifier's Ephemeral Leakage.	115
<i>Łukasz Krzywiecki and Marcin Słowiak</i>	
Evolution of the McEliece Public Key Encryption Scheme.	129
<i>Dominic Bucerzan, Vlad Dragoi, and Hervé Talé Kalachi</i>	
New Algorithm for Modeling S-box in MILP Based Differential and Division Trail Search.	150
<i>Yu Sasaki and Yosuke Todo</i>	

Secretly Embedding Trapdoors into Contract Signing Protocols	166
<i>Diana Maimuț and George Teșeleanu</i>	
On a Key Exchange Protocol	187
<i>Mugurel Barcau, Vicențiu Pașol, Cezar Pleșca, and Mihai Togan</i>	
Author Index	201

Innovative Security Solutions for Information Technology
and Communications

10th International Conference, SecITC 2017, Bucharest,
Romania, June 8–9, 2017, Revised Selected Papers

Farshim, P.; Simion, E. (Eds.)

2017, XII, 201 p. 35 illus., Softcover

ISBN: 978-3-319-69283-8