

Contents

Invited Talks

Circular Security Reconsidered	3
<i>F. Betül Durak and Serge Vaudenay</i>	
Visual Cryptography: Models, Issues, Applications and New Directions. . . .	20
<i>Paolo D'Arco and Roberto De Prisco</i>	
Paper Tigers: An Endless Fight.	40
<i>Mozhdeh Farhadi and Jean-Louis Lanet</i>	
Security of Identity-Based Encryption Schemes from Quadratic Residues. . . .	63
<i>Ferucio Laurențiu Țiplea, Sorin Iftene, George Teșeleanu, and Anca-Maria Nica</i>	

Cryptographic Algorithms and Protocols

Long-Term Secure One-Round Group Key Establishment from Multilinear Mappings.	81
<i>Kashi Neupane</i>	
RSA Weak Public Keys Available on the Internet.	92
<i>Mihai Barbulescu, Adrian Stratulat, Vlad Traista-Popescu, and Emil Simion</i>	
A Tweak for a PRF Mode of a Compression Function and Its Applications . . .	103
<i>Shoichi Hirose and Atsushi Yabumoto</i>	
May-Ozerov Algorithm for Nearest-Neighbor Problem over \mathbb{F}_q and Its Application to Information Set Decoding.	115
<i>Shoichi Hirose</i>	
A Cryptographic Approach for Implementing Semantic Web's Trust Layer. . . .	127
<i>Bogdan Iancu and Cristian Sandu</i>	
Schnorr-Like Identification Scheme Resistant to Malicious Subliminal Setting of Ephemeral Secret	137
<i>Łukasz Krzywiecki</i>	
Homomorphic Encryption Based on Group Algebras and Goldwasser-Micali Scheme.	149
<i>Cezar Pleșca, Mihai Togan, and Cristian Lupașcu</i>	

Increasing the Robustness of the Montgomery <i>kP</i> -Algorithm Against SCA by Modifying Its Initialization	167
<i>Estuardo Alpirez Bock, Zoya Dyka, and Peter Langendoerfer</i>	

Security Technologies for ITC

When Pythons Bite	181
<i>Alecsandru Pătraşcu and Ştefan Popa</i>	

Secure Virtual Machine for Real Time Forensic Tools on Commodity Workstations	193
<i>Dan Luţaş, Adrian Coleşa, Sándor Lukács, and Andrei Luţaş</i>	

Pushing the Optimization Limits of Ring Oscillator-Based True Random Number Generators.	209
<i>Andrei Marghescu and Paul Svasta</i>	

TOR - Didactic Pluggable Transport	225
<i>Ioana-Cristina Panait, Cristian Pop, Alexandru Sirbu, Adelina Vidovici, and Emil Simion</i>	

Preparation of SCA Attacks: Successfully Decapsulating BGA Packages	240
<i>Christian Wittke, Zoya Dyka, Oliver Skibitzki, and Peter Langendoerfer</i>	

Comparative Analysis of Security Operations Centre Architectures; Proposals and Architectural Considerations for Frameworks and Operating Models	248
<i>Sabina Georgiana Radu</i>	

Secure Transaction Authentication Protocol	261
<i>Pardis Pourghomi, Muhammad Qasim Saeed, and Pierre E. Abi-Char</i>	

Proposed Scheme for Data Confidentiality and Access Control in Cloud Computing	274
<i>Ana-Maria Ghimeş and Victor Valeriu Patriciu</i>	

Author Index	287
-------------------------------	-----

Innovative Security Solutions for Information Technology
and Communications

9th International Conference, SECITC 2016, Bucharest,
Romania, June 9-10, 2016, Revised Selected Papers

Bica, I.; Reyhanitabar, R. (Eds.)

2016, X, 287 p. 86 illus., Softcover

ISBN: 978-3-319-47237-9