

Table of Contents

Numerical Semigroups and Bounds on Impossible Differential Attacks on Generalized Feistel Schemes	1
<i>Marina Pudovkina and Alexander Toktarev</i>	
Encrypting Huffman-Encoded Data by Substituting Pairs of Code Words without Changing the Bit Count of a Pair	12
<i>Marek Parfieniuk and Piotr Jankowski</i>	
On Multivariate Cryptosystems Based on Polynomially Compressed Maps with Invertible Decomposition	23
<i>Urszula Romańczuk-Polubiec and Vasyl Ustimenko</i>	
Statistical Analysis of the Chaos-Driven Elliptic Curve Pseudo-Random Number Generators	38
<i>Omar Reyad and Zbigniew Kotulski</i>	
Identity-Based Cryptography in Credit Card Payments	49
<i>Kimmo Hakunen and Mirko Sailio</i>	
On a Cipher Based on Pseudo-random Walks on Graphs	59
<i>Wit Forys, Łukasz Jęda, and Piotr Oprocha</i>	
On LDPC Codes Based on Families of Expanding Graphs of Increasing Girth without Edge-Transitive Automorphism Groups	74
<i>Monika Polak and Vasyl Ustimenko</i>	
Analysis of the Data Flow in the Newscast Protocol for Possible Vulnerabilities	89
<i>Jakub Muszyński, Sébastien Varrette, Juan Luis Jiménez Laredo, and Pascal Bouvry</i>	
Efficient Verifiable Multi-Secret Sharing Based on Y.C.H Scheme	100
<i>Appala Naidu Tentu and Allam Appa Rao</i>	
A Lightweight Authentication Protocol for RFID	110
<i>Ferucio Laurențiu Tiplea</i>	
Long-Term Secure Two-Round Group Key Establishment from Pairings	122
<i>Kashi Neupane</i>	

Optimizing SHA256 in Bitcoin Mining	131
<i>Nicolas T. Courtois, Marek Grajek, and Rahul Naik</i>	
Protocol for Detection of Counterfeit Transactions in Electronic Currency Exchange	145
<i>Marek R. Ogiela and Piotr Sutkowski</i>	
Practical Authentication Protocols for Protecting and Sharing Sensitive Information on Mobile Devices	153
<i>Imed El Fray, Tomasz Hyla, Mirosław Kurkowski, Witold Maćków, and Jerzy Pejaś</i>	
Secure Multihop Key Establishment Protocols for Wireless Sensor Networks	166
<i>Ismail Mansour, Gérard Chalhoub, and Pascal Lafourcade</i>	
Comparison and Assessment of Security Modeling Approaches in Terms of the QoP-ML	178
<i>Katarzyna Mazur and Bogdan Ksiezopolski</i>	
Context-Aware Secure Routing Protocol for Real-Time Services	193
<i>Grzegorz Oryńczak and Zbigniew Kotulski</i>	
Author Index	209