Contents

Symmetric Ciphers

Biclique Attack of Block Cipher SKINNY 3
   Yafei Zheng and Wenling Wu

Improved Differential Cryptanalysis of CAST-128 and CAST-256 18
   Shaomei Wang, Tingting Cui, and Meiqin Wang

Improved Integral and Zero-correlation Linear Cryptanalysis of CLEFIA Block Cipher 33
   Wentan Yi, Baofeng Wu, Shaozhen Chen, and Dongdai Lin

Impossible Differentials of SPN Ciphers 47
   Xuan Shen, Guoqiang Liu, Bing Sun, and Chao Li

SPF: A New Family of Efficient Format-Preserving Encryption Algorithms 64
   Donghoon Chang, Mohona Ghosh, Kishan Chand Gupta, Arpan Jati, Abhishek Kumar, Dukjae Moon, Indranil Ghosh Ray, and Somitra Kumar Sanadhya

Transposition of AES Key Schedule 84
   Jialin Huang, Hailun Yan, and Xuejia Lai

Revisiting the Security Proof of QUAD Stream Cipher: Some Corrections and Tighter Bounds 103
   Goutam Paul and Abhiroop Sanyal

Public-Key Cryptosystems

Achieving IND-CCA Security for Functional Encryption for Inner Products 119
   Shiwei Zhang, Yi Mu, and Guomin Yang

An Improved Analysis on Three Variants of the RSA Cryptosystem 140
   Liqiang Peng, Lei Hu, Yao Lu, and Hongyun Wei

How to Make the Cramer-Shoup Cryptosystem Secure Against Linear Related-Key Attacks 150
   Baodong Qin, Shuai Han, Yu Chen, Shengli Liu, and Zhuo Wei
Signature and Authentication

On Privacy-Preserving Biometric Authentication ............................................. 169
Aysajan Abidin

A Lightweight Authentication and Key Agreement Scheme for Mobile Satellite Communication Systems ................................................................. 187
Xinghua Wu, Aixin Zhang, Jianhua Li, Weiwei Zhao, and Yuchen Liu

Identity-Based Blind Signature from Lattices in Standard Model .................... 205
Wen Gao, Yupu Hu, Baocang Wang, and Jia Xie

Homomorphic Encryption

Multi-bit Leveled Homomorphic Encryption via Dual.LWE-Based ...................... 221
Zengpeng Li, Chunguang Ma, Eduardo Morais, and Gang Du

Cryptanalysis of a Homomorphic Encryption Scheme Over Integers ................. 243
Jingguo Bi, Jiayang Liu, and Xiaoyun Wang

Fully Homomorphic Encryption for Point Numbers ........................................ 253
Seiko Arita and Shota Nakasato

Leakage-Resilient

Bounded-Retrieval Model with Keys Derived from Private Data ........................ 273
Konrad Durnoga, Stefan Dziembowski, Tomasz Kazana, Michał Zając,
and Maciej Zdanowicz

Leakage-Resilient IND-CCA KEM from the Extractable Hash Proofs with Indistinguishability Obfuscation ......................................................... 291
Wenpan Jing, Xianhui Lu, and Bao Li

Codes for Detection of Limited View Algebraic Tampering ............................ 309
Fuchun Lin, Reihaneh Safavi-Naini, and Pengwei Wang

Post-quantum Cryptography

On Fast Calculation of Addition Chains for Isogeny-Based Cryptography ... 323
Brian Koziel, Reza Azarderakhsh, David Jao, and Mehran Mozaffari-Kermani

A Linear Algebra Attack on the Non-commuting Cryptography Class Based on Matrix Power Function ................................................................. 343
Jinhui Liu, Huanguo Zhang, and Jianwei Jia
Commitment and Protocol

Partial Bits Exposure Attacks on a New Commitment Scheme Based on the Zagier Polynomial ................................................................. 357
   Xiaona Zhang and Li-Ping Wang

Key Predistribution Schemes Using Bent Functions in Distributed Sensor Networks .............................................................. 367
   Deepak Kumar Dalai and Pinaki Sarkar

One-Round Cross-Domain Group Key Exchange Protocol in the Standard Model ................................................................. 386
   Xiao Lan, Jing Xu, Hui Guo, and Zhenfeng Zhang

Elliptic Curves

On Constructing Parameterized Families of Pairing-Friendly Elliptic Curves with $\rho = 1$ ................................................. 403
   Meng Zhang, Zhi Hu, and Maozhi Xu

Constructing Isogenies on Extended Jacobi Quartic Curves ............ 416
   Xiu Xu, Wei Yu, Kunpeng Wang, and Xiaoyang He

Security and Implementation

Cyber-Attacks on Remote State Estimation in Industrial Control System: A Game-Based Framework ........................................... 431
   Cong Chen and Dongdai Lin

Secure Collaborative Outsourced k-Nearest Neighbor Classification with Multiple Owners in Cloud Environment ..................... 451
   Hong Rong, Huimei Wang, Jian Liu, Wei Wu, Jialu Hao, and Ming Xian

Video Steganalysis Based on Centralized Error Detection in Spatial Domain .......................................................... 472
   Yu Wang, Yun Cao, and Xianfeng Zhao

Log Your Car: Reliable Maintenance Services Record .................. 484
   Hafizah Mansor, Konstantinos Markantonakis, Raja Naeem Akram, Keith Mayes, and Iakovos Gurulian

Provably Secure Fair Mutual Private Set Intersection Cardinality Utilizing Bloom Filter ...................................................... 505
   Sumit Kumar Debnath and Ratna Dutta

Evaluating Entropy for True Random Number Generators: Efficient, Robust and Provably Secure ........................................... 526
   Maciej Skorski

Author Index ........................................................................... 543
Information Security and Cryptology
12th International Conference, Inscrypt 2016, Beijing, China, November 4-6, 2016, Revised Selected Papers
Chen, K.; Lin, D.; Yung, M. (Eds.)
2017, XIII, 544 p. 78 illus., Softcover
ISBN: 978-3-319-54704-6