Contents

Cryptanalysis of Midori128 Using Impossible Differential Techniques . . . . . 1
Zhan Chen, Huafeng Chen, and Xiaoyun Wang

The Distribution of $2^n$-Periodic Binary Sequences with Fixed $k$-Error
Linear Complexity .................................................. 13
Wenlun Pan, Zhenzhen Bao, Dongdai Lin, and Feng Liu

Cryptanalysis of a Privacy Preserving Auditing for Data Integrity Protocol
from TrustCom 2013 ................................................. 37
Jingguo Bi and Jiayang Liu

A Spark-Based DDoS Attack Detection Model in Cloud Services .............. 48
Jian Zhang, Yawei Zhang, Pin Liu, and Jianbiao He

Security of SM4 Against (Related-Key) Differential Cryptanalysis ............ 65
Jian Zhang, Wenling Wu, and Yafei Zheng

KopperCoin – A Distributed File Storage with Financial Incentives ............ 79
Henning Kopp, Christoph Bösch, and Frank Kargl

Practical Signature Scheme from $I$-Protocol ................................ 94
Zhoujun Ma, Li Yang, and Yunlei Zhao

A Host-Based Detection Method of Remote Access Trojan
in the Early Stage ..................................................... 110
Daichi Adachi and Kazumasa Omote

Collision Attacks on CAESAR Second-Round Candidate: ELmD ............... 122
Jian Zhang, Wenling Wu, and Yafei Zheng

Masking Algorithm for Multiple Crosstalk Attack Source Identification
Under Greedy Sparse Monitoring ...................................... 137
Hong Wei Siew, Saw Chin Tan, and Ching Kwang Lee

Fast Implementation of Simple Matrix Encryption Scheme
on Modern x64 CPU ................................................. 151
Zhiniang Peng, Shaohua Tang, Ju Chen, Chen Wu, and Xinglin Zhang

Homomorphically Encrypted Arithmetic Operations Over the Integer Ring . . 167
Chen Xu, Jingwei Chen, Wenyuan Wu, and Yong Feng

A Privacy Preserving Source Verifiable Encryption Scheme .................... 182
Zhongyuan Yao, Yi Mu, and Guomin Yang
Structural Evaluation for Simon-Like Designs Against Integral Attack

Huiling Zhang and Wenling Wu

RFID Tags Batch Authentication Revisited – Communication Overhead and Server Computational Complexity Limits

Przemysław Błaśkiewicz, Łukasz Krzywiecki, and Piotr Syga

Privacy-Preserving Cloud Auditing with Multiple Uploaders

Ge Wu, Yi Mu, Willy Susilo, and Fuchun Guo

A Formal Concept of Domain Pseudonymous Signatures

Kamil Kluczniak, Lucjan Hanzlik, and Mirosław Kutyłowski

Efficient Tag Path Authentication Protocol with Less Tag Memory

Hongbing Wang, Yingjiu Li, Zongyang Zhang, and Yunlei Zhao

Anonymizing Bitcoin Transaction

Dimaz Ankaa Wijaya, Joseph K. Liu, Ron Steinfeld, Shi-Feng Sun, and Xinyi Huang

Physical-Layer Identification of HF RFID Cards Based on RF Fingerprinting

Guozhu Zhang, Luning Xia, Shijie Jia, and Yafei Ji

Privacy-Preserving Mining of Association Rules for Horizontally Distributed Databases Based on FP-Tree

Yaoan Jin, Chunhua Su, Na Ruan, and Weijia Jia

Countering Burst Header Packet Flooding Attack in Optical Burst Switching Network

Adel Rajab, Chin-Tser Huang, Mohammed Al-Shargabi, and Jorge Cobb

Authenticated CAN Communications Using Standardized Cryptographic Techniques

Zhuo Wei, Yanjiang Yang, and Tieyan Li

Thrifty Zero-Knowledge: When Linear Programming Meets Cryptography

Simon Cogliani, Houda Ferradi, Rémi Géraud, and David Naccache

ARMv8 Shellcodes from ‘A’ to ‘Z’

Hadrien Barral, Houda Ferradi, Rémi Géraud, Georges-Axel Jaloyan, and David Naccache

Author Index

379
Information Security Practice and Experience
12th International Conference, ISPEC 2016, Zhangjiajie, China, November 16-18, 2016, Proceedings
Bao, F.; Chen, L.; Deng, R.H.; Wang, G. (Eds.)
2016, XII, 380 p. 82 illus., Softcover
ISBN: 978-3-319-49150-9