

Contents

Cryptanalysis of Midori128 Using Impossible Differential Techniques	1
<i>Zhan Chen, Huaifeng Chen, and Xiaoyun Wang</i>	
The Distribution of 2^n -Periodic Binary Sequences with Fixed k -Error Linear Complexity	13
<i>Wenlun Pan, Zhenzhen Bao, Dongdai Lin, and Feng Liu</i>	
Cryptanalysis of a Privacy Preserving Auditing for Data Integrity Protocol from TrustCom 2013	37
<i>Jingguo Bi and Jiayang Liu</i>	
A Spark-Based DDoS Attack Detection Model in Cloud Services	48
<i>Jian Zhang, Yawei Zhang, Pin Liu, and Jianbiao He</i>	
Security of SM4 Against (Related-Key) Differential Cryptanalysis	65
<i>Jian Zhang, Wenling Wu, and Yafei Zheng</i>	
KopperCoin – A Distributed File Storage with Financial Incentives	79
<i>Henning Kopp, Christoph Bösch, and Frank Kargl</i>	
Practical Signature Scheme from Γ -Protocol	94
<i>Zhoujun Ma, Li Yang, and Yunlei Zhao</i>	
A Host-Based Detection Method of Remote Access Trojan in the Early Stage	110
<i>Daichi Adachi and Kazumasa Omote</i>	
Collision Attacks on CAESAR Second-Round Candidate: ELMd	122
<i>Jian Zhang, Wenling Wu, and Yafei Zheng</i>	
Masking Algorithm for Multiple Crosstalk Attack Source Identification Under Greedy Sparse Monitoring	137
<i>Hong Wei Siew, Saw Chin Tan, and Ching Kwang Lee</i>	
Fast Implementation of Simple Matrix Encryption Scheme on Modern x64 CPU	151
<i>Zhiniang Peng, Shaohua Tang, Ju Chen, Chen Wu, and Xinglin Zhang</i>	
Homomorphically Encrypted Arithmetic Operations Over the Integer Ring . . .	167
<i>Chen Xu, Jingwei Chen, Wenyuan Wu, and Yong Feng</i>	
A Privacy Preserving Source Verifiable Encryption Scheme	182
<i>Zhongyuan Yao, Yi Mu, and Guomin Yang</i>	

Structural Evaluation for Simon-Like Designs Against Integral Attack	194
<i>Huiling Zhang and Wenling Wu</i>	
RFID Tags Batch Authentication Revisited – Communication Overhead and Server Computational Complexity Limits	209
<i>Przemysław Błażkiewicz, Łukasz Krzywiecki, and Piotr Syga</i>	
Privacy-Preserving Cloud Auditing with Multiple Uploaders.	224
<i>Ge Wu, Yi Mu, Willy Susilo, and Fuchun Guo</i>	
A Formal Concept of Domain Pseudonymous Signatures	238
<i>Kamil Klucznik, Lucjan Hanzlik, and Mirosław Kutylowski</i>	
Efficient Tag Path Authentication Protocol with Less Tag Memory	255
<i>Hongbing Wang, Yingjiu Li, Zongyang Zhang, and Yunlei Zhao</i>	
Anonymizing Bitcoin Transaction	271
<i>Dimaz Ankaa Wijaya, Joseph K. Liu, Ron Steinfeld, Shi-Feng Sun, and Xinyi Huang</i>	
Physical-Layer Identification of HF RFID Cards Based on RF Fingerprinting.	284
<i>Guozhu Zhang, Luning Xia, Shijie Jia, and Yafei Ji</i>	
Privacy-Preserving Mining of Association Rules for Horizontally Distributed Databases Based on FP-Tree	300
<i>Yaoan Jin, Chunhua Su, Na Ruan, and Weijia Jia</i>	
Countering Burst Header Packet Flooding Attack in Optical Burst Switching Network	315
<i>Adel Rajab, Chin-Tser Huang, Mohammed Al-Shargabi, and Jorge Cobb</i>	
Authenticated CAN Communications Using Standardized Cryptographic Techniques	330
<i>Zhuo Wei, Yanjiang Yang, and Tiejian Li</i>	
Thrifty Zero-Knowledge: When Linear Programming Meets Cryptography . . .	344
<i>Simon Cogliani, Houda Ferradi, Rémi Géraud, and David Naccache</i>	
ARMv8 Shellcodes from ‘A’ to ‘Z’	354
<i>Hadrien Barral, Houda Ferradi, Rémi Géraud, Georges-Axel Jaloyan, and David Naccache</i>	
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