

Contents

Minimizing Databases Attack Surface Against SQL Injection Attacks	1
<i>Dimitris Geneiatakis</i>	
Ensuring Kernel Integrity Using KIPBMFH	10
<i>Zhifeng Chen, Qingbao Li, Songhui Guo, and Ye Wang</i>	
Bitsliced Implementations of the PRINCE, LED and RECTANGLE Block Ciphers on AVR 8-Bit Microcontrollers	18
<i>Zhenzhen Bao, Peng Luo, and Dongdai Lin</i>	
On Promise Problem of the Generalized Shortest Vector Problem	37
<i>Wenwen Wang and Kewei Lv</i>	
Secret Key Extraction with Quantization Randomness Using Hadamard Matrix on QuaDRiGa Channel	50
<i>Xuanxuan Wang, Lihuan Jiang, Lars Thiele, and Yongming Wang</i>	
Practical Lattice-Based Fault Attack and Countermeasure on SM2 Signature Algorithm	62
<i>Weiqiong Cao, Jingyi Feng, Shaofeng Zhu, Hua Chen, Wenling Wu, Xucang Han, and Xiaoguang Zheng</i>	
The Security of Polynomial Information of Diffie-Hellman Key	71
<i>Yao Wang and Kewei Lv</i>	
How to Vote Privately Using Bitcoin	82
<i>Zhichao Zhao and T.-H. Hubert Chan</i>	
Multidimensional Zero-Correlation Linear Cryptanalysis on 23-Round LBlock-s	97
<i>Hong Xu, Ping Jia, Geshi Huang, and Xuejia Lai</i>	
Traceable CP-ABE on Prime Order Groups: Fully Secure and Fully Collusion-Resistant Blackbox Traceable	109
<i>Zhen Liu and Duncan S. Wong</i>	
Generic Construction of Audit Logging Schemes with Forward Privacy and Authenticity	125
<i>Shoichi Hirose</i>	
A Novel Post-processing Method to Improve the Ability of Reconstruction for Video Leaking Signal	141
<i>Xuejie Ding, Meng Zhang, Jun Shi, and Weiqing Huang</i>	

TMSUI: A Trust Management Scheme of USB Storage Devices for Industrial Control Systems 152
Bo Yang, Yu Qin, Yingjun Zhang, Weijin Wang, and Dengguo Feng

Characterization of the Third Descent Points for the k -error Linear Complexity of 2^n -periodic Binary Sequences 169
Jianqin Zhou, Wanquan Liu, and Xifeng Wang

QRL: A High Performance Quadruple-Rail Logic for Resisting DPA on FPGA Implementations 184
Chenyang Tu, Jian Zhou, Neng Gao, Zeyi Liu, Yuan Ma, and Zongbin Liu

Strategy of Relations Collection in Factoring RSA Modulus 199
Haibo Yu and Guoqiang Bai

Ultra High-Performance ASIC Implementation of SM2 with SPA Resistance 212
Dan Zhang and Guoqiang Bai

Multi-input Functional Encryption and Its Application in Outsourcing Computation 220
Peili Li, Haixia Xu, and Yuanyuan Ji

A Multivariate Encryption Scheme with Rainbow 236
Takanori Yasuda and Kouichi Sakurai

Efficient and Secure Many-to-One Signature Delegation 252
Rajeev Anand Sahu and Vishal Saraswat

Fully Secure IBE with Tighter Reduction in Prime Order Bilinear Groups . . . 260
Jie Zhang, Aijun Ge, Siyu Xiao, and Chuangui Ma

A Secure Route Optimization Mechanism for Expressive Internet Architecture (XIA) Mobility 269
Hongwei Meng, Zhong Chen, Ziqian Meng, and Chuck Song

An Entropy Based Encrypted Traffic Classifier 282
Mohammad Saiful Islam Mamun, Ali A. Ghorbani, and Natalia Stakhanova

Modelling and Analysis of Network Security - a Probabilistic Value-passing CCS Approach 295
Qian Zhang, Ying Jiang, and Liping Ding

An Improved NPCUSUM Method with Adaptive Sliding Window to Detect DDoS Attacks 303
Degang Sun, Kun Yang, Weiqing Huang, Yan Wang, and Bo Hu

Dynamic Hybrid Honeypot System Based Transparent Traffic
Redirection Mechanism 311
Wenjun Fan, Zhihui Du, David Fernández, and Xinning Hui

Leveraging Static Probe Instrumentation for VM-based Anomaly Detection
System 320
*Ady Wahyudi Paundu, Takeshi Okuda, Youki Kadobayashi,
and Suguru Yamaguchi*

MB-DDIVR: A Map-Based Dynamic Data Integrity Verification
and Recovery Scheme in Cloud Storage. 335
Zizhou Sun, Yahui Yang, Qingni Shen, Zhonghai Wu, and Xiaochen Li

Chameleon: A Lightweight Method for Thwarting Relay Attacks
in Near Field Communication. 346
*Yafei Ji, Luning Xia, Jingqiang Lin, Jian Zhou, Guozhu Zhang,
and Shijie Jia*

A Solution of Code Authentication on Android. 356
Xue Zhang and Rui Zhang

Verifiable Proxy Re-encryption from Indistinguishability Obfuscation 363
Muhua Liu, Ying Wu, Jinyong Chang, Rui Xue, and Wei Guo

Higher-Order Masking Schemes for SIMON 379
Jiehui Tang, Yongbin Zhou, Hailong Zhang, and Shuang Qiu

An ORAM Scheme with Improved Worst-Case Computational Overhead. 393
Nairen Cao, Xiaoqi Yu, Yufang Yang, Linru Zhang, and SiuMing Yiu

A Self-Matching Sliding Block Algorithm Applied to Deduplication
in Distributed Storage System. 406
Chuiyi Xie, Ying Huo, Sihan Qing, Shoushan Luo, and Lingli Hu

Suffix Type String Matching Algorithms Based on Multi-windows
and Integer Comparison 414
Hongbo Fan, Shupeng Shi, Jing Zhang, and Li Dong

Security-Enhanced Reprogramming with XORs Coding in Wireless
Sensor Networks. 421
Depeng Chen, Daojing He, and Sammy Chan

Preserving Context Privacy in Distributed Hash Table Wireless
Sensor Networks. 436
Paolo Palmieri

Prior Classification of Stego Containers as a New Approach for Enhancing
Steganalyzers Accuracy 445
Viktor Monarev and Andrey Pestunov

Eavesdropper: A Framework for Detecting the Location of the Processed Result in Hadoop 458
Chuntao Dong, Qingni Shen, Wenting Li, Yahui Yang, Zhonghai Wu, and Xiang Wan

Secret Picture: An Efficient Tool for Mitigating Deletion Delay on OSN 467
Shangqi Lai, Joseph K. Liu, Kim-Kwang Raymond Choo, and Kaitai Liang

A De-anonymization Attack on Geo-Located Data Considering Spatio-temporal Influences 478
Rong Wang, Min Zhang, Dengguo Feng, Yanyan Fu, and Zhenyu Chen

Author Index 485



<http://www.springer.com/978-3-319-29813-9>

Information and Communications Security
17th International Conference, ICICS 2015, Beijing,
China, December 9-11, 2015, Revised Selected Papers
Qing, S.; Okamoto, E.; Kim, K.; Liu, D. (Eds.)
2016, XVIII, 486 p. 133 illus. in color., Softcover
ISBN: 978-3-319-29813-9