

# 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
<i>Bo Yang, Yu Qin, Yingjun Zhang, Weijin Wang, and Dengguo Feng</i>	
Characterization of the Third Descent Points for the $k$ -error Linear Complexity of $2^n$ -periodic Binary Sequences . . . . .	169
<i>Jianqin Zhou, Wanquan Liu, and Xifeng Wang</i>	
QRL: A High Performance Quadruple-Rail Logic for Resisting DPA on FPGA Implementations . . . . .	184
<i>Chenyang Tu, Jian Zhou, Neng Gao, Zeyi Liu, Yuan Ma, and Zongbin Liu</i>	
Strategy of Relations Collection in Factoring RSA Modulus . . . . .	199
<i>Haibo Yu and Guoqiang Bai</i>	
Ultra High-Performance ASIC Implementation of SM2 with SPA Resistance . . . . .	212
<i>Dan Zhang and Guoqiang Bai</i>	
Multi-input Functional Encryption and Its Application in Outsourcing Computation . . . . .	220
<i>Peili Li, Haixia Xu, and Yuanyuan Ji</i>	
A Multivariate Encryption Scheme with Rainbow . . . . .	236
<i>Takanori Yasuda and Kouichi Sakurai</i>	
Efficient and Secure Many-to-One Signature Delegation . . . . .	252
<i>Rajeev Anand Sahu and Vishal Saraswat</i>	
Fully Secure IBE with Tighter Reduction in Prime Order Bilinear Groups . . .	260
<i>Jie Zhang, Aijun Ge, Siyu Xiao, and Chuangui Ma</i>	
A Secure Route Optimization Mechanism for Expressive Internet Architecture (XIA) Mobility . . . . .	269
<i>Hongwei Meng, Zhong Chen, Ziqian Meng, and Chuck Song</i>	
An Entropy Based Encrypted Traffic Classifier . . . . .	282
<i>Mohammad Saiful Islam Mamun, Ali A. Ghorbani, and Natalia Stakhanova</i>	
Modelling and Analysis of Network Security - a Probabilistic Value-passing CCS Approach. . . . .	295
<i>Qian Zhang, Ying Jiang, and Liping Ding</i>	
An Improved NPCUSUM Method with Adaptive Sliding Window to Detect DDoS Attacks. . . . .	303
<i>Degang Sun, Kun Yang, Weiqing Huang, Yan Wang, and Bo Hu</i>	

Dynamic Hybrid Honeypot System Based Transparent Traffic Redirection Mechanism . . . . .	311
<i>Wenjun Fan, Zhihui Du, David Fernández, and Xinning Hui</i>	
Leveraging Static Probe Instrumentation for VM-based Anomaly Detection System . . . . .	320
<i>Ady Wahyudi Paundu, Takeshi Okuda, Youki Kadobayashi, and Suguru Yamaguchi</i>	
MB-DDIVR: A Map-Based Dynamic Data Integrity Verification and Recovery Scheme in Cloud Storage. . . . .	335
<i>Zizhou Sun, Yahui Yang, Qingni Shen, Zhonghai Wu, and Xiaochen Li</i>	
Chameleon: A Lightweight Method for Thwarting Relay Attacks in Near Field Communication. . . . .	346
<i>Yafei Ji, Luning Xia, Jingqiang Lin, Jian Zhou, Guozhu Zhang, and Shijie Jia</i>	
A Solution of Code Authentication on Android. . . . .	356
<i>Xue Zhang and Rui Zhang</i>	
Verifiable Proxy Re-encryption from Indistinguishability Obfuscation . . . . .	363
<i>Muhua Liu, Ying Wu, Jinyong Chang, Rui Xue, and Wei Guo</i>	
Higher-Order Masking Schemes for SIMON . . . . .	379
<i>Jiehui Tang, Yongbin Zhou, Hailong Zhang, and Shuang Qiu</i>	
An ORAM Scheme with Improved Worst-Case Computational Overhead. . . . .	393
<i>Nairen Cao, Xiaoqi Yu, Yufang Yang, Linru Zhang, and SiuMing Yiu</i>	
A Self-Matching Sliding Block Algorithm Applied to Deduplication in Distributed Storage System. . . . .	406
<i>Chuiyi Xie, Ying Huo, Sihan Qing, Shoushan Luo, and Lingli Hu</i>	
Suffix Type String Matching Algorithms Based on Multi-windows and Integer Comparison. . . . .	414
<i>Hongbo Fan, Shupeng Shi, Jing Zhang, and Li Dong</i>	
Security-Enhanced Reprogramming with XORs Coding in Wireless Sensor Networks. . . . .	421
<i>Depeng Chen, Daojing He, and Sammy Chan</i>	
Preserving Context Privacy in Distributed Hash Table Wireless Sensor Networks. . . . .	436
<i>Paolo Palmieri</i>	
Prior Classification of Stego Containers as a New Approach for Enhancing Steganalyzers Accuracy . . . . .	445
<i>Viktor Monarev and Andrey Pestunov</i>	

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

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