Contents

Digital Signatures

A General Framework for Redactable Signatures and New Constructions 3
David Derler, Henrich C. Pöhls, Kai Samelin, and Daniel Slamanig

On the Security of the Schnorr Signature Scheme and DSA Against Related-Key Attacks 20
Hiraku Morita, Jacob C.N. Schuldt, Takahiro Matsuda, Goichiro Hanaoka, and Tetsu Iwata

Attribute-Based Two-Tier Signatures: Definition and Construction 36
Hiroaki Anada, Seiko Arita, and Kouichi Sakurai

Public-Key Cryptography

Ciphertext-Policy Attribute-Based Broadcast Encryption with Small Keys . . . 53
Benjamin Wesolowski and Pascal Junod

Learning with Errors in the Exponent 69
Özgür Dagdelen, Sebastian Gajek, and Florian Göpfert

Block Cipher Cryptanalysis

Higher-Order Cryptanalysis of LowMC 87
Christoph Dobraunig, Maria Eichlseder, and Florian Mendel

Integral Attack Against Bit-Oriented Block Ciphers 102
Huiling Zhang, Wenling Wu, and Yanfeng Wang

Single Key Recovery Attacks on 9-Round Kalyna-128/256 and Kalyna-256/512 119
Akshima, Donghoon Chang, Mohona Ghosh, Aarushi Goel, and Somitra Kumar Sanadhya

Improved Impossible Differential Attack on Reduced-Round LBlock 136
Ning Wang, Xiaoyun Wang, and Keting Jia

Elliptic Curve Cryptography

Point Decomposition Problem in Binary Elliptic Curves 155
Koray Karabina

Faster ECC over $\mathbb{F}_{2^{521}-1}$ (feat. NEON) 169
Hwajeong Seo, Zhe Liu, Yasuyuki Nogami, Taehwan Park, Jongseok Choi, Lu Zhou, and Howon Kim

Protocols

On the (In)Efficiency of Non-Interactive Secure Multiparty Computation 185
Maki Yoshida and Satoshi Obana

Apollo: End-to-End Verifiable Voting Protocol Using Mixnet and Hidden Tweaks 194
Donghoon Chang, Amit Kumar Chauhan, Muhammed Noufal K, and Jinkeon Kang

On Differentially Private Online Collaborative Recommendation Systems . . . 210
Seth Gilbert, Xiao Liu, and Haifeng Yu

Security

Stack Layout Randomization with Minimal Rewriting of Android Binaries. . . 229
Yu Liang, Xinjie Ma, Daoyuan Wu, Xiaoxiao Tang, Debin Gao, Guojun Peng, Chunfu Jia, and Huanguo Zhang

Improving Fuzzing Using Software Complexity Metrics 246
Maksim O. Shudrak and Vyacheslav V. Zolotarev

Uncloaking Rootkits on Mobile Devices with a Hypervisor-Based Detector. . . . 262
Julian Vetter, Matthias Junker-Petschick, Jan Nordholz, Michael Peter, and Janis Danisevskis

Detecting Obfuscated Suspicious JavaScript Based on Information-Theoretic Measures and Novelty Detection 278
Jiawei Su, Katsunari Yoshioka, Junji Shikata, and Tsutomu Matsumoto

Side-Channel Attacks

Two Lattice-Based Differential Fault Attacks Against ECDSA with *w*NAF Algorithm 297
Weiqiong Cao, Jingyi Feng, Hua Chen, Shaofeng Zhu, Wenling Wu, Xucang Han, and Xiaoguang Zheng

Maximum Likelihood-Based Key Recovery Algorithm from Decayed Key Schedules 314
Tomoyuki Tanigaki and Noboru Kunihiro

New Efficient Padding Methods Secure Against Padding Oracle Attacks 329
HyungChul Kang, Myungseo Park, Dukjae Moon, Changhoon Lee, Jongsung Kim, Kimoon Kim, Juhyuk Kim, and Seokhie Hong

Physical Unclonable Functions

Let Me Prove It to You: RO PUFs Are Provably Learnable 345
Fatemeh Ganji, Shahin Tajik, and Jean-Pierre Seifert

Anonymous Authentication Scheme Based on PUF 359
Łukasz Krzywiecki

Author Index 373

http://www.springer.com/978-3-319-30839-5

Information Security and Cryptology - ICISC 2015
18th International Conference, Seoul, South Korea,
November 25-27, 2015, Revised Selected Papers
Kwon, S.; Yun, A. (Eds.)
2016, XIII, 374 p. 62 illus. in color., Softcover
ISBN: 978-3-319-30839-5