Contents

Identity-Based Encryption

Identity-Based Lossy Encryption from Learning with Errors 3
Jingnan He, Bao Li, Xianhui Lu, Dingding Jia, Haiyang Xue, and Xiaochao Sun

Adaptive-ID Secure Revocable Hierarchical Identity-Based Encryption 21
Jae Hong Seo and Keita Emura

Elliptic Curve Cryptography

Invalid Curve Attacks in a GLS Setting 41
Taechan Kim and Mehdi Tibouchi

New Fast Algorithms for Elliptic Curve Arithmetic in Affine Coordinates . . . 56
Wei Yu, Kwang Ho Kim, and Myong Song Jo

Factoring

Implicit Factorization of RSA Moduli Revisited (Short Paper) 67
Liqiang Peng, Lei Hu, Yao Lu, Zhangjie Huang, and Jun Xu

Symmetric Cryptanalysis

Improved (Pseudo) Preimage Attacks on Reduced-Round GOST and Grøstl-256 and Studies on Several Truncation Patterns for AES-like Compression Functions 79
Bingke Ma, Bao Li, Ronglin Hao, and Xiaoqian Li

Improvement on the Method for Automatic Differential Analysis and Its Application to Two Lightweight Block Ciphers DESL and LBlock-s 97
Siwei Sun, Lei Hu, Kexin Qiao, Xiaoshuang Ma, Jinyong Shan, and Ling Song

Provable Security

NM-CPA Secure Encryption with Proofs of Plaintext Knowledge 115
Ben Smyth, Yoshikazu Hanatani, and Hirofumi Muratani

Improvement of UC Secure Searchable Symmetric Encryption Scheme 135
Shunsuke Taketani and Wakaha Ogata

Fully Leakage-Resilient Non-malleable Identification Schemes in the Bounded-Retrieval Model. 153
Tingting Zhang and Hongda Li

LWE-Based Encryption

LWE-Based FHE with Better Parameters 175
Fuqun Wang, Kunpeng Wang, and Bao Li

Improved Efficiency of MP12. 193
Fuyang Fang, Bao Li, Xianhui Lu, and Xiaochao Sun

Secret Sharing

Almost Optimum Secret Sharing Schemes with Cheating Detection for Random Bit Strings 213
Hidetaka Hoshino and Satoshi Obana

Privacy-Preserving and Anonymity

k-Anonymous Microdata Release via Post Randomisation Method. 225
Dai Ikarashi, Ryo Kikuchi, Koji Chida, and Katsumi Takahashi

On Limitations and Alternatives of Privacy-Preserving Cryptographic Protocols for Genomic Data 242
Tadanori Teruya, Koji Nuida, Kana Shimizu, and Goichiro Hanaoka

Anonymous Credential System with Efficient Proofs for Monotone Formulas on Attributes 262
Shahidatul Sadiah, Toru Nakanishi, and Nobuo Funabiki

Secure Protocol

Secure Multi-Party Computation Using Polarizing Cards 281
Kazumasa Shinagawa, Takaaki Mizuki, Jacob Schuldt, Koji Nuida, Naoki Kanayama, Takashi Nishide, Goichiro Hanaoka, and Eiji Okamoto

Systems Security

An Analysis Platform for the Information Security of In-Vehicle Networks Connected with External Networks 301
Takaya Ezaki, Tomohiro Date, and Hiroyuki Inoue

Beyond Scale: An Efficient Framework for Evaluating Web Access Control Policies in the Era of Big Data 316
Tong Liu and Yazhe Wang

Artifact-Metric-Based Authentication for Bottles of Wine (Short Paper) 335
Reina Yagasaki and Kazuo Sakiyama

Security in Hardware

Bit Error Probability Evaluation of Ring Oscillator PUF (Short Paper) 347
Qinglong Zhang, Zongbin Liu, Cunqing Ma, and Jiwu Jing

Author Index 357



http://www.springer.com/978-3-319-22424-4

Advances in Information and Computer Security
10th International Workshop on Security, IWSEC 2015,
Nara, Japan, August 26-28, 2015, Proceedings
Tanaka, K.; Suga, Y. (Eds.)
2015, XIII, 357 p. 51 illus., Softcover
ISBN: 978-3-319-22424-4