Liqun Chen · Jinguang Han (Eds.)

Provable Security

10th International Conference, ProvSec 2016 Nanjing, China, November 10–11, 2016 Proceedings

Springer

Contents

Attribute/Role-Based Cryptography

Accountable Ciphertext-Policy Attribute-Based Encryption Scheme Supporting Public Verifiability and Nonrepudiation 3
Gang Yu, Zhenfu Cao, Guang Zeng, and Wenbao Han

An Efficient and Expressive Ciphertext-Policy Attribute-Based Encryption Scheme with Partially Hidden Access Structures 19
Hui Cui, Robert H. Deng, Guowei Wu, and Junzuo Lai

Ciphertext-Policy Attribute Based Encryption Supporting Access Policy Update 39
Yinhao Jiang, Willy Susilo, Yi Mu, and Fuchun Guo

Universally Composable Cryptographic Role-Based Access Control 61
Bin Liu and Bogdan Warinschi

Data in Cloud

ID-based Data Integrity Auditing Scheme from RSA with Resisting Key Exposure 83
Jianhong Zhang, Pengyan Li, Zhibin Sun, and Jian Mao

Efficient Dynamic Provable Data Possession from Dynamic Binary Tree 101
Changfeng Li and Huaqun Wang

Identity-Based Batch Provable Data Possession 112
Fucai Zhou, Su Peng, Jian Xu, and Zifeng Xu

Secure Naïve Bayesian Classification over Encrypted Data in Cloud 130
Xingxin Li, Youwen Zhu, and Jian Wang

Searchable Encryption

Integrity Preserving Multi-keyword Searchable Encryption for Cloud Computing 153
Fucai Zhou, Yuxi Li, Alex X. Liu, Muqing Lin, and Zifeng Xu

Oblivious Keyword Search with Authorization 173
Peng Jiang, Xiaofen Wang, Jianchang Lai, Fuchun Guo, and Rongmao Chen

Efficient Asymmetric Index Encapsulation Scheme for Named Data 191
Rong Ma and Zhenfu Cao

Key Management

Multi-cast Key Distribution: Scalable, Dynamic and Provably Secure Construction 207
Kazuki Yoneyama, Reo Yoshida, Yuto Kawahara, Tetsutaro Kobayashi, Hitoshi Fuji, and Tomohide Yamamoto

One-Round Attribute-Based Key Exchange in the Multi-party Setting 227
Yangguang Tian, Guomin Yang, Yi Mu, Kaitai Liang, and Yong Yu

Strongly Secure Two-Party Certificateless Key Agreement Protocol with Short Message 244
Yong Xie, Libing Wu, Yubo Zhang, and Zhiyan Xu

Encryption

Integrity Analysis of Authenticated Encryption Based on Stream Ciphers 257
Kazuya Imamura, Kazuhiko Minematsu, and Tetsu Iwata

Secure and Efficient Construction of Broadcast Encryption with Dealership . . . 277
Kamalesh Acharya and Ratna Dutta

Towards Certificate-Based Group Encryption 296
Yili Ren, Xiling Luo, Qianhong Wu, Joseph K. Liu, and Peng Zhang

Leakage Analysis

Updatable Lossy Trapdoor Functions and Its Application in Continuous Leakage 309
Sujuan Li, Yi Mu, Mingwu Zhang, and Futai Zhang

A Black-Box Construction of Strongly Unforgeable Signature Schemes in the Bounded Leakage Model 320
Jianye Huang, Qiong Huang, and Chunhua Pan

Towards Proofs of Ownership Beyond Bounded Leakage 340
Yongjun Zhao and Sherman S.M. Chow

Homomorphic Encryption

A Homomorphic Proxy Re-encryption from Lattices 353
Chunguang Ma, Juyan Li, and Weiping Ouyang

Preventing Adaptive Key Recovery Attacks on the GSW Levelled Homomorphic Encryption Scheme 373
Zengpeng Li, Steven D. Galbraith, and Chunguang Ma

A Secure Reverse Multi-Attribute First-Price E-Auction Mechanism Using Multiple Auctioneer Servers (Work in Progress) 384
Jun Gao, Jiaqi Wang, Ning Lu, Fang Zhu, and Wenbo Shi

Author Index 393