

Contents

Attribute/Role-Based Cryptography

Accountable Ciphertext-Policy Attribute-Based Encryption Scheme Supporting Public Verifiability and Nonrepudiation	3
<i>Gang Yu, Zhenfu Cao, Guang Zeng, and Wenbao Han</i>	
An Efficient and Expressive Ciphertext-Policy Attribute-Based Encryption Scheme with Partially Hidden Access Structures	19
<i>Hui Cui, Robert H. Deng, Guowei Wu, and Junzuo Lai</i>	
Ciphertext-Policy Attribute Based Encryption Supporting Access Policy Update.	39
<i>Yinhao Jiang, Willy Susilo, Yi Mu, and Fuchun Guo</i>	
Universally Composable Cryptographic Role-Based Access Control	61
<i>Bin Liu and Bogdan Warinschi</i>	

Data in Cloud

ID-based Data Integrity Auditing Scheme from RSA with Resisting Key Exposure	83
<i>Jianhong Zhang, Pengyan Li, Zhibin Sun, and Jian Mao</i>	
Efficient Dynamic Provable Data Possession from Dynamic Binary Tree	101
<i>Changfeng Li and Huaqun Wang</i>	
Identity-Based Batch Provable Data Possession.	112
<i>Fucui Zhou, Su Peng, Jian Xu, and Zifeng Xu</i>	
Secure Naïve Bayesian Classification over Encrypted Data in Cloud	130
<i>Xingxin Li, Youwen Zhu, and Jian Wang</i>	

Searchable Encryption

Integrity Preserving Multi-keyword Searchable Encryption for Cloud Computing	153
<i>Fucui Zhou, Yuxi Li, Alex X. Liu, Muqing Lin, and Zifeng Xu</i>	
Oblivious Keyword Search with Authorization	173
<i>Peng Jiang, Xiaofen Wang, Jianchang Lai, Fuchun Guo, and Rongmao Chen</i>	

Efficient Asymmetric Index Encapsulation Scheme for Named Data	191
<i>Rong Ma and Zhenfu Cao</i>	

Key Management

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

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

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

Encryption

Integrity Analysis of Authenticated Encryption Based on Stream Ciphers . . .	257
<i>Kazuya Imamura, Kazuhiko Minematsu, and Tetsu Iwata</i>	

Secure and Efficient Construction of Broadcast Encryption with Dealership . .	277
<i>Kamalesh Acharya and Ratna Dutta</i>	

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

Leakage Analysis

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

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

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

Homomorphic Encryption

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

Preventing Adaptive Key Recovery Attacks on the GSW Levelled Homomorphic Encryption Scheme	373
<i>Zengpeng Li, Steven D. Galbraith, and Chunguang Ma</i>	
A Secure Reverse Multi-Attribute First-Price E-Auction Mechanism Using Multiple Auctioneer Servers (Work in Progress)	384
<i>Jun Gao, Jiaqi Wang, Ning Lu, Fang Zhu, and Wenbo Shi</i>	
Author Index	393

Provable Security

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

Chen, L.; Han, J. (Eds.)

2016, XIII, 394 p. 34 illus., Softcover

ISBN: 978-3-319-47421-2