

Contents – Part II

Signature and Key Management

| | |
|--|----|
| One-Round Strong Oblivious Signature-Based Envelope | 3 |
| <i>Rongmao Chen, Yi Mu, Willy Susilo, Guomin Yang, Fuchun Guo, and Mingwu Zhang</i> | |
| Proxy Signature with Revocation | 21 |
| <i>Shengmin Xu, Guomin Yang, Yi Mu, and Sha Ma</i> | |
| On the Relations Between Security Notions in Hierarchical Key Assignment Schemes for Dynamic Structures | 37 |
| <i>Arcangelo Castiglione, Alfredo De Santis, Barbara Masucci, Francesco Palmieri, and Aniello Castiglione</i> | |

Public Key and Identity-Based Encryption

| | |
|--|-----|
| Content-Based Encryption | 57 |
| <i>Xiaofen Wang and Yi Mu</i> | |
| Provably Secure Threshold Paillier Encryption Based on Hyperplane Geometry | 73 |
| <i>Zhe Xia, Xiaoyun Yang, Min Xiao, and Debiao He</i> | |
| Identity-Based Group Encryption | 87 |
| <i>Xiling Luo, Yili Ren, Jingwen Liu, Jiankun Hu, Weiran Liu, Zhen Wang, Wei Xu, and Qianhong Wu</i> | |
| Edit Distance Based Encryption and Its Application | 103 |
| <i>Tran Viet Xuan Phuong, Guomin Yang, Willy Susilo, and Kaitai Liang</i> | |
| Proxy Re-encryption with Delegatable Verifiability | 120 |
| <i>Xiaodong Lin and Rongxing Lu</i> | |
| Efficient Completely Non-Malleable and RKA Secure Public Key Encryptions | 134 |
| <i>Shi-Feng Sun, Udaya Parampalli, Tsz Hon Yuen, Yu Yu, and Dawu Gu</i> | |

Searchable Encryption

| | |
|--|-----|
| Verifiable Searchable Encryption with Aggregate Keys for Data Sharing in Outsourcing Storage | 153 |
| <i>Tong Li, Zheli Liu, Ping Li, Chunfu Jia, Zoe L. Jiang, and Jin Li</i> | |
| Public Key Encryption with Authorized Keyword Search. | 170 |
| <i>Peng Jiang, Yi Mu, Fuchun Guo, and Qiaoyan Wen</i> | |
| Linear Encryption with Keyword Search | 187 |
| <i>Shiwei Zhang, Guomin Yang, and Yi Mu</i> | |

Broadcast Encryption

| | |
|---|-----|
| Generic Anonymous Identity-Based Broadcast Encryption with Chosen-Ciphertext Security | 207 |
| <i>Kai He, Jian Weng, Man Ho Au, Yijun Mao, and Robert H. Deng</i> | |
| Anonymous Identity-Based Broadcast Encryption with Revocation for File Sharing | 223 |
| <i>Jianchang Lai, Yi Mu, Fuchun Guo, Willy Susilo, and Rongmao Chen</i> | |

Mathematical Primitives

| | |
|--|-----|
| Partial Key Exposure Attacks on RSA with Multiple Exponent Pairs. | 243 |
| <i>Atsushi Takayasu and Noboru Kunihiro</i> | |
| A New Attack on Three Variants of the RSA Cryptosystem. | 258 |
| <i>Martin Bunder, Abderrahmane Nitaj, Willy Susilo, and Joseph Tonien</i> | |
| Generalized Hardness Assumption for Self-bilinear Map with Auxiliary Information | 269 |
| <i>Takashi Yamakawa, Goichiro Hanaoka, and Noboru Kunihiro</i> | |
| Deterministic Encoding into Twisted Edwards Curves | 285 |
| <i>Wei Yu, Kunpeng Wang, Bao Li, Xiaoyang He, and Song Tian</i> | |

Symmetric Cipher

| | |
|---|-----|
| Improved Rebound Attacks on AESQ: Core Permutation of CAESAR Candidate PAEQ. | 301 |
| <i>Nasour Bagheri, Florian Mendel, and Yu Sasaki</i> | |
| Efficient Beyond-Birthday-Bound-Secure Deterministic Authenticated Encryption with Minimal Stretch. | 317 |
| <i>Christian Forler, Eik List, Stefan Lucks, and Jakob Wenzel</i> | |

| | |
|---|-----|
| Improved (related-key) Attacks on Round-Reduced KATAN-32/48/64 Based on the Extended Boomerang Framework | 333 |
| <i>Jiageng Chen, Je Sen Teh, Chunhua Su, Azman Samsudin, and Junbin Fang</i> | |
| Authenticated Encryption with Small Stretch (or, How to Accelerate AERO) | 347 |
| <i>Kazuhiko Minematsu</i> | |
| Impossible Differential Cryptanalysis of 14-Round Camellia-192 | 363 |
| <i>Keting Jia and Ning Wang</i> | |
| Automatic Differential Analysis of ARX Block Ciphers with Application to SPECK and LEA | 379 |
| <i>Ling Song, Zhangjie Huang, and Qianqian Yang</i> | |
| On the Security of the LAC Authenticated Encryption Algorithm | 395 |
| <i>Jiqiang Lu</i> | |
| Linear Hull Attack on Round-Reduced Simeck with Dynamic Key-Guessing Techniques | 409 |
| <i>Lingyue Qin, Huaifeng Chen, and Xiaoyun Wang</i> | |
| Short Papers-Public Key and Identity-Based Encryption | |
| Reducing the Key Size of the SRP Encryption Scheme | 427 |
| <i>Dung Hoang Duong, Albrecht Petzoldt, and Tsuyoshi Takagi</i> | |
| Short Papers-Biometric Security | |
| Biometric Access Control with High Dimensional Facial Features. | 437 |
| <i>Ying Han Pang, Ean Yee Khor, and Shih Yin Ooi</i> | |
| Security Analysis on Privacy-Preserving Cloud Aided Biometric Identification Schemes. | 446 |
| <i>Shiran Pan, Shen Yan, and Wen-Tao Zhu</i> | |
| Short Papers-Digital Forensics | |
| Interest Profiling for Security Monitoring and Forensic Investigation. | 457 |
| <i>Min Yang, Fei Xu, and Kam-Pui Chow</i> | |
| Short Papers-National Security Infrastructure | |
| Pseudonymous Signature on eIDAS Token – Implementation Based Privacy Threats. | 467 |
| <i>Miroslaw Kutylowski, Lucjan Hanzlik, and Kamil Kluczniak</i> | |

Short Papers-Mobile Security

| | |
|--|-----|
| A Feasible No-Root Approach on Android. | 481 |
| <i>Yao Cheng, Yingjiu Li, and Robert H. Deng</i> | |

Short Papers-Network Security

| | |
|--|-----|
| Improved Classification of Known and Unknown Network Traffic Flows Using Semi-supervised Machine Learning | 493 |
| <i>Timothy Glennan, Christopher Leckie, and Sarah M. Erfani</i> | |

Short Papers-Pseudo Random/One-way Function

| | |
|--|-----|
| A Noiseless Key-Homomorphic PRF: Application on Distributed Storage Systems | 505 |
| <i>Jhordany Rodriguez Parra, Terence Chan, and Siu-Wai Ho</i> | |

| | |
|-------------------------------|-----|
| Author Index | 515 |
|-------------------------------|-----|

Contents – Part I

Invited Papers

| | |
|---|----|
| I Know Where You All Are! Exploiting Mobile Social Apps for Large-Scale Location Privacy Probing | 3 |
| <i>Shuang Zhao, Xiapu Luo, Bo Bai, Xiaobo Ma, Wei Zou, Xinliang Qiu, and Man Ho Au</i> | |
| MUSE: Towards Robust and Stealthy Mobile Botnets via Multiple Message Push Services | 20 |
| <i>Wei Chen, Xiapu Luo, Chengyu Yin, Bin Xiao, Man Ho Au, and Yajuan Tang</i> | |
| A Survey on the Cyber Attacks Against Non-linear State Estimation in Smart Grids | 40 |
| <i>Jingxuan Wang, Lucas C.K. Hui, S.M. Yiu, Xingmin Cui, Eric Ke Wang, and Junbin Fang</i> | |
| Towards Bitcoin Payment Networks | 57 |
| <i>Patrick McCorry, Malte Möser, Siamak F. Shahandasti, and Feng Hao</i> | |
| Statistical Disclosure Control for Data Privacy Using Sequence of Generalised Linear Models | 77 |
| <i>Min Cherng Lee, Robin Mitra, Emmanuel Lazaridis, An Chow Lai, Yong Kheng Goh, and Wun-She Yap</i> | |
| Energy-Efficient Elliptic Curve Cryptography for MSP430-Based Wireless Sensor Nodes | 94 |
| <i>Zhe Liu, Johann Großschädl, Lin Li, and Qiuliang Xu</i> | |

National Security Infrastructure

| | |
|---|-----|
| A Comparison Study of Wireless Network Security in Several Australasian Cities and Suburbs | 115 |
| <i>Alastair Nisbet and Andrew Woodward</i> | |
| On the Guessability of Resident Registration Numbers in South Korea | 128 |
| <i>Youngbae Song, Hyounghshick Kim, and Jun Ho Huh</i> | |

Social Network Security

| | |
|--|-----|
| Towards Privacy-Preserving Data Mining in Online Social Networks: Distance-Grained and Item-Grained Differential Privacy. | 141 |
| <i>Shen Yan, Shiran Pan, Yuhang Zhao, and Wen-Tao Zhu</i> | |

Bitcoin Security

| | |
|---|-----|
| Fair Client Puzzles from the Bitcoin Blockchain | 161 |
| <i>Colin Boyd and Christopher Carr</i> | |

Statistical Privacy

| | |
|--|-----|
| Privacy-Preserving k -Nearest Neighbour Query on Outsourced Database | 181 |
| <i>Rui Xu, Kirill Morozov, Yanjiang Yang, Jianying Zhou, and Tsuyoshi Takagi</i> | |
| Reversible Data Hiding for Encrypted Images Based on Statistical Learning . . . | 198 |
| <i>Zhen Li and Wei Wu</i> | |

Network Security

| | |
|--|-----|
| An Ensemble Learning Approach for Addressing the Class Imbalance Problem in Twitter Spam Detection. | 215 |
| <i>Shigang Liu, Yu Wang, Chao Chen, and Yang Xiang</i> | |

Smart City Security

| | |
|---|-----|
| Putting the User in Control of the Intelligent Transportation System | 231 |
| <i>Catalin Gosman, Tudor Cornea, Ciprian Dobre, Florin Pop, and Aniello Castiglione</i> | |

Digital Forensics

| | |
|--|-----|
| Exploring the Space of Digital Evidence – Position Paper | 249 |
| <i>Carsten Rudolph</i> | |

Lightweight Security

| | |
|--|-----|
| Towards Lightweight Anonymous Entity Authentication for IoT Applications. | 265 |
| <i>Yanjiang Yang, Haibin Cai, Zhuo Wei, Haibing Lu, and Kim-Kwang Raymond Choo</i> | |
| Hybrid MQ Signature for Embedded Device | 281 |
| <i>Shaohua Tang, Bo Lv, and Wuqiang Shen</i> | |

Secure Batch Processing

| | |
|--|-----|
| Batch Verifiable Computation with Public Verifiability for Outsourcing Polynomials and Matrix Computations. | 293 |
| <i>Yujuan Sun, Yu Yu, Xiangxue Li, Kai Zhang, Haifeng Qian, and Yuan Zhou</i> | |
| Accelerating Oblivious Transfer with Batch Multi-exponentiation | 310 |
| <i>Yang Sun, Qianhong Wu, Jingwen Liu, Jianwei Liu, Xinyi Huang, Bo Qin, and Wei Hu</i> | |

Pseudo Random/One-way Function

| | |
|---|-----|
| CTM-sp: A Family of Cryptographic Hash Functions from Chaotic Tent Maps. | 329 |
| <i>Xun Yi, Xuechao Yang, Yong Feng, Fengling Han, and Ron van Schyndel</i> | |
| One-Key Compression Function Based MAC with Security Beyond Birthday Bound | 343 |
| <i>Avijit Dutta, Mridul Nandi, and Goutam Paul</i> | |

Cloud Storage Security

| | |
|---|-----|
| Towards Efficient Fully Randomized Message-Locked Encryption | 361 |
| <i>Tao Jiang, Xiaofeng Chen, Qianhong Wu, Jianfeng Ma, Willy Susilo, and Wenjing Lou</i> | |
| Secure and Traceable Framework for Data Circulation. | 376 |
| <i>Kaitai Liang, Atsuko Miyaji, and Chunhua Su</i> | |
| Public Cloud Data Auditing with Practical Key Update and Zero Knowledge Privacy | 389 |
| <i>Yong Yu, Yannan Li, Man Ho Au, Willy Susilo, Kim-Kwang Raymond Choo, and Xinpeng Zhang</i> | |

Password/QR Code Security

| | |
|--|-----|
| Exploiting the Error Correction Mechanism in QR Codes for Secret Sharing | 409 |
| <i>Yang-Wai Chow, Willy Susilo, Guomin Yang, James G. Phillips, Ilung Pranata, and Ari Moesriami Barmawi</i> | |
| Password Requirements Markup Language. | 426 |
| <i>Moritz Horsch, Mario Schlipf, Johannes Braun, and Johannes Buchmann</i> | |

Functional Encryption and Attribute-Based Cryptosystem

| | |
|---|-----|
| Leakage-Resilient Functional Encryption via Pair Encodings | 443 |
| <i>Zuoxia Yu, Man Ho Au, Qiuliang Xu, Rupeng Yang, and Jinguang Han</i> | |
| Secret Handshakes with Dynamic Expressive Matching Policy | 461 |
| <i>Lin Hou, Junzuo Lai, and Lixian Liu</i> | |
| Ciphertext-Policy Attribute-Based Encryption with Key-Delegation Abuse Resistance | 477 |
| <i>Yinhao Jiang, Willy Susilo, Yi Mu, and Fuchun Guo</i> | |
| Chosen Ciphertext Secure Attribute-Based Encryption with Outsourced Decryption | 495 |
| <i>Cong Zuo, Jun Shao, Guiyi Wei, Mande Xie, and Min Ji</i> | |
| Accountable Large-Universe Attribute-Based Encryption Supporting Any Monotone Access Structures. | 509 |
| <i>Yinghui Zhang, Jin Li, Dong Zheng, Xiaofeng Chen, and Hui Li</i> | |
| A Cloud-Based Access Control Scheme with User Revocation and Attribute Update | 525 |
| <i>Peng Zhang, Zehong Chen, Kaitai Liang, Shulan Wang, and Ting Wang</i> | |
| Author Index | 541 |

Information Security and Privacy

21st Australasian Conference, ACISP 2016, Melbourne,
VIC, Australia, July 4-6, 2016, Proceedings, Part II

Liu, J.K.; Steinfeld, R. (Eds.)

2016, XVIII, 517 p. 46 illus., Softcover

ISBN: 978-3-319-40366-3