Contents – Part II

Signature and Key Management

One-Round Strong Oblivious Signature-Based Envelope .......................... 3
   Rongmao Chen, Yi Mu, Willy Susilo, Guomin Yang, Fuchun Guo,
   and Mingwu Zhang

Proxy Signature with Revocation ............................................................ 21
   Shengmin Xu, Guomin Yang, Yi Mu, and Sha Ma

On the Relations Between Security Notions in Hierarchical Key
Assignment Schemes for Dynamic Structures ........................................... 37
   Arcangelo Castiglione, Alfredo De Santis, Barbara Masucci,
   Francesco Palmieri, and Aniello Castiglione

Public Key and Identity-Based Encryption

Content-Based Encryption ................................................................. 57
   Xiaofen Wang and Yi Mu

Provably Secure Threshold Paillier Encryption Based on Hyperplane
Geometry ..................................................................................................... 73
   Zhe Xia, Xiaoyun Yang, Min Xiao, and Debiao He

Identity-Based Group Encryption ............................................................ 87
   Xiling Luo, Yili Ren, Jingwen Liu, Jiankun Hu, Weiran Liu,
   Zhen Wang, Wei Xu, and Qianhong Wu

Edit Distance Based Encryption and Its Application ............................... 103
   Tran Viet Xuan Phuong, Guomin Yang, Willy Susilo, and Kaitai Liang

Proxy Re-encryption with Delegatable Verifiability ................................. 120
   Xiaodong Lin and Rongxing Lu

Efficient Completely Non-Malleable and RKA Secure Public Key
Encryptions .............................................................................................. 134
   Shi-Feng Sun, Udaya Parampalli, Tsz Hon Yuen, Yu Yu, and Dawu Gu
Searchable Encryption

Verifiable Searchable Encryption with Aggregate Keys for Data Sharing in Outsourcing Storage ......................................................... 153
   Tong Li, Zheli Liu, Ping Li, Chunfu Jia, Zoe L. Jiang, and Jin Li

Public Key Encryption with Authorized Keyword Search ............... 170
   Peng Jiang, Yi Mu, Fuchun Guo, and Qiaoyan Wen

Linear Encryption with Keyword Search ................................... 187
   Shiwei Zhang, Guomin Yang, and Yi Mu

Broadcast Encryption

Generic Anonymous Identity-Based Broadcast Encryption with Chosen-Ciphertext Security ......................................................... 207
   Kai He, Jian Weng, Man Ho Au, Yijun Mao, and Robert H. Deng

Anonymous Identity-Based Broadcast Encryption with Revocation for File Sharing ................................................................. 223
   Jianchang Lai, Yi Mu, Fuchun Guo, Willy Susilo, and Rongmao Chen

Mathematical Primitives

Partial Key Exposure Attacks on RSA with Multiple Exponent Pairs .................. 243
   Atsushi Takayasu and Noboru Kunihiro

A New Attack on Three Variants of the RSA Cryptosystem .................. 258
   Martin Bunder, Abderrahmane Nitaj, Willy Susilo, and Joseph Tonien

Generalized Hardness Assumption for Self-bilinear Map with Auxiliary Information ............................................................... 269
   Takashi Yamakawa, Goichiro Hanaoka, and Noboru Kunihiro

Deterministic Encoding into Twisted Edwards Curves ....................... 285
   Wei Yu, Kunpeng Wang, Bao Li, Xiaoyang He, and Song Tian

Symmetric Cipher

Improved Rebound Attacks on AESQ: Core Permutation of CAESAR Candidate PAEQ ................................................................. 301
   Nasour Bagheri, Florian Mendel, and Yu Sasaki

Efficient Beyond-Birthday-Bound-Secure Deterministic Authenticated Encryption with Minimal Stretch ............................... 317
   Christian Forler, Eik List, Stefan Lucks, and Jakob Wenzel
Improved (related-key) Attacks on Round-Reduced KATAN-32/48/64 Based on the Extended Boomerang Framework

Jiageng Chen, Je Sen Teh, Chunhua Su, Azman Samsudin, and Junbin Fang

Authenticated Encryption with Small Stretch (or, How to Accelerate AERO)

Kazuhiko Minematsu

Impossible Differential Cryptanalysis of 14-Round Camellia-192

Keting Jia and Ning Wang

Automatic Differential Analysis of ARX Block Ciphers with Application to SPECK and LEA

Ling Song, Zhangjie Huang, and Qianqian Yang

On the Security of the LAC Authenticated Encryption Algorithm

Jiqiang Lu

Linear Hull Attack on Round-Reduced Simeck with Dynamic Key-Guessing Techniques

Lingyue Qin, Huaiieng Chen, and Xiaoyun Wang

Short Papers—Public Key and Identity-Based Encryption

Reducing the Key Size of the SRP Encryption Scheme

Dung Hoang Duong, Albrecht Petzoldt, and Tsuyoshi Takagi

Short Papers—Biometric Security

Biometric Access Control with High Dimensional Facial Features

Ying Han Pang, Ean Yee Khor, and Shih Yin Ooi

Security Analysis on Privacy-Preserving Cloud Aided Biometric Identification Schemes

Shiran Pan, Shen Yan, and Wen-Tao Zhu

Short Papers—Digital Forensics

Interest Profiling for Security Monitoring and Forensic Investigation

Min Yang, Fei Xu, and Kam-Pui Chow

Short Papers—National Security Infrastructure

Pseudonymous Signature on eIDAS Token – Implementation Based Privacy Threats

Mirosław Kutyłowski, Lucjan Hanzlik, and Kamil KluczniaK
Short Papers-Mobile Security

A Feasible No-Root Approach on Android. 481
Yao Cheng, Yingjiu Li, and Robert H. Deng

Short Papers-Network Security

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

Short Papers-Pseudo Random/One-way Function

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

Author Index 515
Contents – Part I

Invited Papers

I Know Where You All Are! Exploiting Mobile Social Apps for Large-Scale Location Privacy Probing
Shuang Zhao, Xiapu Luo, Bo Bai, Xiaobo Ma, Wei Zou, Xinliang Qiu, and Man Ho Au

MUSE: Towards Robust and Stealthy Mobile Botnets via Multiple Message Push Services
Wei Chen, Xiapu Luo, Chengyu Yin, Bin Xiao, Man Ho Au, and Yajuan Tang

A Survey on the Cyber Attacks Against Non-linear State Estimation in Smart Grids
Jingxuan Wang, Lucas C.K. Hui, S.M. Yiu, Xingmin Cui, Eric Ke Wang, and Junbin Fang

Towards Bitcoin Payment Networks
Patrick McCorry, Malte Möser, Siamak F. Shahandasti, and Feng Hao

Statistical Disclosure Control for Data Privacy Using Sequence of Generalised Linear Models
Min Cherng Lee, Robin Mitra, Emmanuel Lazaridis, An Chow Lai, Yong Kheng Goh, and Wun-She Yap

Energy-Efficient Elliptic Curve Cryptography for MSP430-Based Wireless Sensor Nodes
Zhe Liu, Johann Großschädl, Lin Li, and Qiuliang Xu

National Security Infrastructure

A Comparison Study of Wireless Network Security in Several Australasian Cities and Suburbs
Alastair Nisbet and Andrew Woodward

On the Guessability of Resident Registration Numbers in South Korea
Youngbae Song, Hyoungshick Kim, and Jun Ho Huh
Contents – Part I

Social Network Security
Towards Privacy-Preserving Data Mining in Online Social Networks:
Distance-Grained and Item-Grained Differential Privacy
Shen Yan, Shiran Pan, Yuhang Zhao, and Wen-Tao Zhu

Bitcoin Security
Fair Client Puzzles from the Bitcoin Blockchain
Colin Boyd and Christopher Carr

Statistical Privacy
Privacy-Preserving $k$-Nearest Neighbour Query on Outsourced Database
Rui Xu, Kirill Morozov, Yanjiang Yang, Jianying Zhou, and Tsuyoshi Takagi
Reversible Data Hiding for Encrypted Images Based on Statistical Learning
Zhen Li and Wei Wu

Network Security
An Ensemble Learning Approach for Addressing the Class Imbalance Problem in Twitter Spam Detection
Shigang Liu, Yu Wang, Chao Chen, and Yang Xiang

Smart City Security
Putting the User in Control of the Intelligent Transportation System
Catalin Gosman, Tudor Cornea, Ciprian Dobre, Florin Pop, and Aniello Castiglione

Digital Forensics
Exploring the Space of Digital Evidence – Position Paper
Carsten Rudolph

Lightweight Security
Towards Lightweight Anonymous Entity Authentication for IoT Applications
Yanjiang Yang, Haibin Cai, Zhuo Wei, Haibing Lu, and Kim-Kwang Raymond Choo

Hybrid MQ Signature for Embedded Device
Shaohua Tang, Bo Lv, and Wuqiang Shen
Secure Batch Processing

Batch Verifiable Computation with Public Verifiability for Outsourcing
Polynomials and Matrix Computations ................................................. 293
  Yujuan Sun, Yu Yu, Xiangxue Li, Kai Zhang, Haifeng Qian,
  and Yuan Zhou

Accelerating Oblivious Transfer with Batch Multi-exponentiation .......... 310
  Yang Sun, Qianhong Wu, Jingwen Liu, Jianwei Liu, Xinyi Huang,
  Bo Qin, and Wei Hu

Pseudo Random/One-way Function

CTM-sp: A Family of Cryptographic Hash Functions from Chaotic Tent
Maps ................................................................................................. 329
  Xun Yi, Xuechao Yang, Yong Feng, Fengling Han,
  and Ron van Schyndel

One-Key Compression Function Based MAC with Security Beyond
Birthday Bound .................................................................................. 343
  Avijit Dutta, Mridul Nandi, and Goutam Paul

Cloud Storage Security

Towards Efficient Fully Randomized Message-Locked Encryption .......... 361
  Tao Jiang, Xiaofeng Chen, Qianhong Wu, Jianfeng Ma, Willy Susilo,
  and Wenjing Lou

Secure and Traceable Framework for Data Circulation ......................... 376
  Kaitai Liang, Atsuko Miyaji, and Chunhua Su

Public Cloud Data Auditing with Practical Key Update and Zero
Knowledge Privacy ............................................................................ 389
  Yong Yu, Yannan Li, Man Ho Au, Willy Susilo,
  Kim-Kwang Raymond Choo, and Xinpeng Zhang

Password/QR Code Security

Exploiting the Error Correction Mechanism in QR Codes for Secret Sharing . . 409
  Yang-Wai Chow, Willy Susilo, Guomin Yang, James G. Phillips,
  Ilung Pranata, and Ari Moesriami Barmawi

Password Requirements Markup Language ....................................... 426
  Moritz Horsch, Mario Schlipf, Johannes Braun,
  and Johannes Buchmann
<table>
<thead>
<tr>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Functional Encryption and Attribute-Based Cryptosystem</td>
<td>443</td>
</tr>
<tr>
<td>Leakage-Resilient Functional Encryption via Pair Encodings</td>
<td></td>
</tr>
<tr>
<td>Zuoxia Yu, Man Ho Au, Qiuliang Xu, Rupeng Yang, and Jinguang Han</td>
<td>443</td>
</tr>
<tr>
<td>Secret Handshakes with Dynamic Expressive Matching Policy</td>
<td>461</td>
</tr>
<tr>
<td>Lin Hou, Junzuo Lai, and Lixian Liu</td>
<td>461</td>
</tr>
<tr>
<td>Ciphertext-Policy Attribute-Based Encryption with Key-Delegation Abuse Resistance</td>
<td>477</td>
</tr>
<tr>
<td>Yinhao Jiang, Willy Susilo, Yi Mu, and Fuchun Guo</td>
<td>477</td>
</tr>
<tr>
<td>Chosen Ciphertext Secure Attribute-Based Encryption with Outsourced Decryption</td>
<td>495</td>
</tr>
<tr>
<td>Cong Zuo, Jun Shao, Guiyi Wei, Mande Xie, and Min Ji</td>
<td>495</td>
</tr>
<tr>
<td>Accountable Large-Universe Attribute-Based Encryption Supporting Any Monotone Access Structures</td>
<td>509</td>
</tr>
<tr>
<td>Yinghui Zhang, Jin Li, Dong Zheng, Xiaofeng Chen, and Hui Li</td>
<td>509</td>
</tr>
<tr>
<td>A Cloud-Based Access Control Scheme with User Revocation and Attribute Update</td>
<td>525</td>
</tr>
<tr>
<td>Peng Zhang, Zehong Chen, Kaitai Liang, Shulan Wang, and Ting Wang</td>
<td>525</td>
</tr>
<tr>
<td><strong>Author Index</strong></td>
<td>541</td>
</tr>
</tbody>
</table>
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