Contents – Part II

Symmetric Cryptography

Analysis of Toeplitz MDS Matrices
Sumanta Sarkar and Habeeb Syed

Reforgeability of Authenticated Encryption Schemes
Christian Forler, Eik List, Stefan Lucks, and Jakob Wenzel

Indifferentiability of Double-Block-Length Hash Function Without Feed-Forward Operations
Yusuke Naito

Software Security

FFFuzzer: Filter Your Fuzz to Get Accuracy, Efficiency and Schedulability
Fan Jiang, Cen Zhang, and Shaoyin Cheng

Splitting Third-Party Libraries’ Privileges from Android Apps
Jiawei Zhan, Quan Zhou, Xiaozhuo Gu, Yuewu Wang, and Yingjiao Niu

SafeStack+: Enhanced Dual Stack to Combat Data-Flow Hijacking
Yan Lin, Xiaoxiao Tang, and Debin Gao

Network Security

Prover Efficient Public Verification of Dense or Sparse/Structured Matrix-Vector Multiplication
Jean-Guillaume Dumas and Vincent Zucca

JSFfox: Run-Timely Confining JavaScript for Firefox
Weizhong Qiang, JiaZhen Guo, Hai Jin, and Weifeng Li

Malware Detection

PriMal: Cloud-Based Privacy-Preserving Malware Detection
Hao Sun, Jinshu Su, Xiaofeng Wang, Rongmao Chen, Yujing Liu, and Qiaolin Hu

A New Malware Classification Approach Based on Malware Dynamic Analysis
Ying Fang, Bo Yu, Yong Tang, Liu Liu, Zexin Lu, Yi Wang, and Qiang Yang
Privacy

Privacy-Preserving Aggregation of Time-Series Data with Public
Verifiability from Simple Assumptions ........................................ 193

Keita Emura

Privacy-Utility Tradeoff for Applications Using Energy Disaggregation
of Smart-Meter Data .................................................................... 214

Mitsuhiro Hattori, Takato Hirano, Nori Matsuda, Rina Shimizu,
and Ye Wang

Private Graph Intersection Protocol ............................................. 235

Fucai Zhou, Zifeng Xu, Yuxi Li, Jian Xu, and Su Peng

Computing Aggregates Over Numeric Data with Personalized
Local Differential Privacy ............................................................... 249

Mousumi Akter and Tanzima Hashem

An Efficient Toolkit for Computing Private Set Operations ............... 261

Alex Davidson and Carlos Cid

Authentication

Privacy-Preserving k-time Authenticated Secret Handshakes ............... 281

Yangguang Tian, Shiwei Zhang, Guomin Yang, Yi Mu, and Yong Yu

Exploring Effect of Location Number on Map-Based Graphical
Password Authentication ................................................................. 301

Weizhi Meng, Wang Hao Lee, Man Ho Au, and Zhe Liu

A QR Code Watermarking Approach Based on the DWT-DCT Technique... 314

Yang-Wai Chow, Willy Susilo, Joseph Tonien, and Wei Zong

Elliptic Curve Cryptography

Generating Complete Edwards Curves ......................................... 335

Theo Fanuela Prabowo and Chik How Tan

Secure GLS Recomposition for Sum-of-Square Cofactors ............... 349

Eunkyung Kim and Mehdi Tibouchi

Differential Addition on Twisted Edwards Curves ............................. 366

Reza Rezaeian Farashahi and Seyed Gholamhossein Hosseini
Short Papers

Certificate Transparency with Enhancements and Short Proofs ................ 381
   Abhishek Singh, Binanda Sengupta, and Sushmita Ruj

Update-Tolerant and Revocable Password Backup ......................... 390
   Moritz Horsch, Johannes Braun, Dominique Metz, and Johannes Buchmann

Redactable Graph Hashing, Revisited (Extended Abstract) ............... 398
   Andreas Erwig, Marc Fischlin, Martin Hald, Dominik Helm, Robert Kiel, Florian Kübler, Michael Kümerlin, Jakob Laenge, and Felix Rohrbach

On the Security of Designing a Cellular Automata Based Stream Cipher ... 406
   Swapan Maiti, Shamit Ghosh, and Dipanwita Roy Chowdhury

Stegogames .................................................. 414
   Clark Thomborson and Marc Jeanmougin

A Feasibility Evaluation of Fair and Privacy-Enhanced Matchmaking with Identity Linked Wishes ...................................................... 422
   Dwight Horne and Suku Nair

Fully Context-Sensitive CFI for COTS Binaries .......................... 435
   Weizhong Qiang, Yingda Huang, Deqing Zou, Hai Jin, Shizhen Wang, and Guozhong Sun

Dual-Mode Cryptosystem Based on the Learning with Errors Problem .......... 443
   Jingnan He, Wenpan Jing, Bao Li, Xianhui Lu, and Dingding Jia

Process Control Cyber-Attacks and Labelled Datasets on S7Comm Critical Infrastructure ............................................................. 452
   Nicholas R. Rodofile, Thomas Schmidt, Sebastian T. Sherry, Christopher Djamaludin, Kenneth Radke, and Ernest Foo

Solving the DLP with Low Hamming Weight Product Exponents and Improved Attacks on the GPS Identification Scheme ....................... 460
   Jason H.M. Ying and Noboru Kunihiro

Author Index ...................................................... 469
Contents – Part I

Public Key Encryption

Tightly-Secure Encryption in the Multi-user, Multi-challenge Setting with Improved Efficiency ........................................ 3
Puwen Wei, Wei Wang, Bingxin Zhu, and Siu Ming Yiu

Hierarchical Functional Encryption for Linear Transformations ............. 23
Shiwei Zhang, Yi Mu, Guomin Yang, and Xiaofen Wang

KDM-Secure Public-Key Encryption from Constant-Noise LPN ............. 44
Shuai Han and Shengli Liu

Long-Term Secure Commitments via Extractable-Binding Commitments .... 65
Ahto Buldas, Matthias Geihs, and Johannes Buchmann

Attribute-Based Encryption

New Proof Techniques for DLIN-Based Adaptively Secure
Attribute-Based Encryption ............................................. 85
Katsuyuki Takashima

Attribute-Based Encryption with Expressive and Authorized
Keyword Search ......................................................... 106
Hui Cui, Robert H. Deng, Joseph K. Liu, and Yingjiu Li

Towards Revocable Fine-Grained Encryption of Cloud Data:
Reducing Trust upon Cloud ............................................ 127
Yanjiang Yang, Joseph Liu, Zhuo Wei, and Xinyi Huang

Identity-Based Encryption

Mergeable and Revocable Identity-Based Encryption .......................... 147
Shengmin Xu, Guomin Yang, Yi Mu, and Willy Susilo

ID-Based Encryption with Equality Test Against Insider Attack ............ 168
Tong Wu, Sha Ma, Yi Mu, and Shengke Zeng

Lattice-Based Revocable Identity-Based Encryption with Bounded
Decryption Key Exposure Resistance .................................. 184
Atsushi Takayasu and Yohei Watanabe
## Searchable Encryption

Dynamic Searchable Symmetric Encryption with Physical Deletion and Small Leakage

Peng Xu, Shuai Liang, Wei Wang, Willy Susilo, Qianhong Wu, and Hai Jin

Multi-user Cloud-Based Secure Keyword Search

Shabnam Kasra Kermanshahi, Joseph K. Liu, and Ron Steinfeld

Fuzzy Keyword Search and Access Control over Ciphertexts in Cloud Computing

Hong Zhu, Zhuolin Mei, Bing Wu, Hongbo Li, and Zongmin Cui

Secure and Practical Searchable Encryption: A Position Paper

Shujie Cui, Muhammad Rizwan Asghar, Steven D. Galbraith, and Giovanni Russello

## Cryptanalysis

Fault Attacks on XEX Mode with Application to Certain Authenticated Encryption Modes

Hassan Qahur Al Mahri, Leonie Simpson, Harry Bartlett, Ed Dawson, and Kenneth Koon-Ho Wong

How to Handle Rainbow Tables with External Memory

Gildas Avoine, Xavier Carpent, Barbara Kordy, and Florent Tardif

Improved Factoring Attacks on Multi-prime RSA with Small Prime Difference

Mengce Zheng, Noboru Kunihiro, and Honggang Hu

Efficient Compilers for After-the-Fact Leakage: From CPA to CCA-2 Secure PKE to AKE

Suvradip Chakraborty, Goutam Paul, and C. Pandu Rangan

Improved Integral Attack on HIGHT

Yuki Funabiki, Yosuke Todo, Takanori Isobe, and Masakatu Morii

Cryptanalysis of Simpira v2

Ivan Tjuawinata, Tao Huang, and Hongjun Wu

Statistical Integral Distinguisher with Multi-structure and Its Application on AES

Tingting Cui, Ling Sun, Huafeng Chen, and Meiqin Wang

Conditional Differential Cryptanalysis for Kreyvium

Yuhei Watanabe, Takanori Isobe, and Masakatu Morii
Digital Signatures

Practical Strongly Invisible and Strongly Accountable Sanitizable Signatures .................................................. 437

  Michael Till Beck, Jan Camenisch, David Derler, Stephan Krenn,
  Henrich C. Pöhls, Kai Samelin, and Daniel Slamanig

Tightly-Secure Signatures from the Decisional Composite Residuosity Assumption ........................................... 453

  Xiao Zhang, Shengli Liu, and Dawu Gu

Author Index ................................................................. 469
Information Security and Privacy
Pieprzyk, J.; Suriadi, S. (Eds.)
2017, XVII, 471 p. 93 illus., Softcover
ISBN: 978-3-319-59869-7