

Contents – Part I

Public Key Encryption

Tightly-Secure Encryption in the Multi-user, Multi-challenge Setting with Improved Efficiency.	3
<i>Puwen Wei, Wei Wang, Bingxin Zhu, and Siu Ming Yiu</i>	
Hierarchical Functional Encryption for Linear Transformations	23
<i>Shiwei Zhang, Yi Mu, Guomin Yang, and Xiaofen Wang</i>	
KDM-Secure Public-Key Encryption from Constant-Noise LPN	44
<i>Shuai Han and Shengli Liu</i>	
Long-Term Secure Commitments via Extractable-Binding Commitments	65
<i>Ahto Buldas, Matthias Geihs, and Johannes Buchmann</i>	

Attribute-Based Encryption

New Proof Techniques for DLIN-Based Adaptively Secure Attribute-Based Encryption.	85
<i>Katsuyuki Takashima</i>	
Attribute-Based Encryption with Expressive and Authorized Keyword Search	106
<i>Hui Cui, Robert H. Deng, Joseph K. Liu, and Yingjiu Li</i>	
Towards Revocable Fine-Grained Encryption of Cloud Data: Reducing Trust upon Cloud	127
<i>Yanjiang Yang, Joseph Liu, Zhuo Wei, and Xinyi Huang</i>	

Identity-Based Encryption

Mergeable and Revocable Identity-Based Encryption	147
<i>Shengmin Xu, Guomin Yang, Yi Mu, and Willy Susilo</i>	
ID-Based Encryption with Equality Test Against Insider Attack	168
<i>Tong Wu, Sha Ma, Yi Mu, and Shengke Zeng</i>	
Lattice-Based Revocable Identity-Based Encryption with Bounded Decryption Key Exposure Resistance.	184
<i>Atsushi Takayasu and Yohei Watanabe</i>	

Searchable Encryption

Dynamic Searchable Symmetric Encryption with Physical Deletion and Small Leakage	207
<i>Peng Xu, Shuai Liang, Wei Wang, Willy Susilo, Qianhong Wu, and Hai Jin</i>	
Multi-user Cloud-Based Secure Keyword Search.	227
<i>Shabnam Kasra Kermanshahi, Joseph K. Liu, and Ron Steinfeld</i>	
Fuzzy Keyword Search and Access Control over Ciphertexts in Cloud Computing	248
<i>Hong Zhu, Zhuolin Mei, Bing Wu, Hongbo Li, and Zongmin Cui</i>	
Secure and Practical Searchable Encryption: A Position Paper	266
<i>Shujie Cui, Muhammad Rizwan Asghar, Steven D. Galbraith, and Giovanni Russello</i>	

Cryptanalysis

Fault Attacks on XEX Mode with Application to Certain Authenticated Encryption Modes.	285
<i>Hassan Qahur Al Mahri, Leonie Simpson, Harry Bartlett, Ed Dawson, and Kenneth Koon-Ho Wong</i>	
How to Handle Rainbow Tables with External Memory.	306
<i>Gildas Avoine, Xavier Carpent, Barbara Kordy, and Florent Tardif</i>	
Improved Factoring Attacks on Multi-prime RSA with Small Prime Difference.	324
<i>Mengce Zheng, Noboru Kunihiro, and Honggang Hu</i>	
Efficient Compilers for After-the-Fact Leakage: From CPA to CCA-2 Secure PKE to AKE.	343
<i>Suvradip Chakraborty, Goutam Paul, and C. Pandu Rangan</i>	
Improved Integral Attack on HIGHT.	363
<i>Yuki Funabiki, Yosuke Todo, Takanori Isobe, and Masakatu Morii</i>	
Cryptanalysis of Simpira v2	384
<i>Ivan Tjuawinata, Tao Huang, and Hongjun Wu</i>	
Statistical Integral Distinguisher with Multi-structure and Its Application on AES	402
<i>Tingting Cui, Ling Sun, Huaifeng Chen, and Meiqin Wang</i>	
Conditional Differential Cryptanalysis for Kreyvium	421
<i>Yuhei Watanabe, Takanori Isobe, and Masakatu Morii</i>	

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

Contents – Part II

Symmetric Cryptography

Analysis of Toeplitz MDS Matrices.	3
<i>Sumanta Sarkar and Habeeb Syed</i>	
Reforgeability of Authenticated Encryption Schemes	19
<i>Christian Forler, Eik List, Stefan Lucks, and Jakob Wenzel</i>	
Indifferentiability of Double-Block-Length Hash Function Without Feed-Forward Operations.	38
<i>Yusuke Naito</i>	

Software Security

FFFuzzer: Filter Your Fuzz to Get Accuracy, Efficiency and Schedulability . . .	61
<i>Fan Jiang, Cen Zhang, and Shaoyin Cheng</i>	
Splitting Third-Party Libraries' Privileges from Android Apps	80
<i>Jiawei Zhan, Quan Zhou, Xiaozhuo Gu, Yuewu Wang, and Yingjiao Niu</i>	
SafeStack ⁺ : Enhanced Dual Stack to Combat Data-Flow Hijacking	95
<i>Yan Lin, Xiaoxiao Tang, and Debin Gao</i>	

Network Security

Prover Efficient Public Verification of Dense or Sparse/Structured Matrix-Vector Multiplication	115
<i>Jean-Guillaume Dumas and Vincent Zucca</i>	
JSFfox: Run-Timely Confining JavaScript for Firefox	135
<i>Weizhong Qiang, JiaZhen Guo, Hai Jin, and Weifeng Li</i>	

Malware Detection

PriMal: Cloud-Based Privacy-Preserving Malware Detection.	153
<i>Hao Sun, Jinshu Su, Xiaofeng Wang, Rongmao Chen, Yujing Liu, and Qiaolin Hu</i>	
A New Malware Classification Approach Based on Malware Dynamic Analysis.	173
<i>Ying Fang, Bo Yu, Yong Tang, Liu Liu, Zexin Lu, Yi Wang, and Qiang Yang</i>	

Privacy

Privacy-Preserving Aggregation of Time-Series Data with Public Verifiability from Simple Assumptions	193
<i>Keita Emura</i>	
Privacy-Utility Tradeoff for Applications Using Energy Disaggregation of Smart-Meter Data	214
<i>Mitsuhiro Hattori, Takato Hirano, Nori Matsuda, Rina Shimizu, and Ye Wang</i>	
Private Graph Intersection Protocol	235
<i>Fucaï Zhou, Zifeng Xu, Yuxi Li, Jian Xu, and Su Peng</i>	
Computing Aggregates Over Numeric Data with Personalized Local Differential Privacy	249
<i>Mousumi Akter and Tanzima Hashem</i>	
An Efficient Toolkit for Computing Private Set Operations	261
<i>Alex Davidson and Carlos Cid</i>	

Authentication

Privacy-Preserving k-time Authenticated Secret Handshakes	281
<i>Yangguang Tian, Shiwei Zhang, Guomin Yang, Yi Mu, and Yong Yu</i>	
Exploring Effect of Location Number on Map-Based Graphical Password Authentication	301
<i>Weizhi Meng, Wang Hao Lee, Man Ho Au, and Zhe Liu</i>	
A QR Code Watermarking Approach Based on the DWT-DCT Technique. . .	314
<i>Yang-Wai Chow, Willy Susilo, Joseph Tonien, and Wei Zong</i>	

Elliptic Curve Cryptography

Generating Complete Edwards Curves	335
<i>Theo Fanuela Prabowo and Chik How Tan</i>	
Secure GLS Recomposition for Sum-of-Square Cofactors.	349
<i>Eunkyung Kim and Mehdi Tibouchi</i>	
Differential Addition on Twisted Edwards Curves	366
<i>Reza Rezaeian Farashahi and Seyed Gholamhossein Hosseini</i>	

Short Papers

Certificate Transparency with Enhancements and Short Proofs	381
<i>Abhishek Singh, Binanda Sengupta, and Sushmita Ruj</i>	
Update-Tolerant and Revocable Password Backup.	390
<i>Moritz Horsch, Johannes Braun, Dominique Metz, and Johannes Buchmann</i>	
Redactable Graph Hashing, Revisited (Extended Abstract)	398
<i>Andreas Erwig, Marc Fischlin, Martin Hald, Dominik Helm, Robert Kiel, Florian Kübler, Michael Kümmerlin, Jakob Laenge, and Felix Rohrbach</i>	
On the Security of Designing a Cellular Automata Based Stream Cipher	406
<i>Swapan Maiti, Shamit Ghosh, and Dipanwita Roy Chowdhury</i>	
Stegogames	414
<i>Clark Thomborson and Marc Jeanmougin</i>	
A Feasibility Evaluation of Fair and Privacy-Enhanced Matchmaking with Identity Linked Wishes.	422
<i>Dwight Horne and Suku Nair</i>	
Fully Context-Sensitive CFI for COTS Binaries	435
<i>Weizhong Qiang, Yingda Huang, Deqing Zou, Hai Jin, Shizhen Wang, and Guozhong Sun</i>	
Dual-Mode Cryptosystem Based on the Learning with Errors Problem.	443
<i>Jingnan He, Wenpan Jing, Bao Li, Xianhui Lu, and Dingding Jia</i>	
Process Control Cyber-Attacks and Labelled Datasets on S7Comm Critical Infrastructure.	452
<i>Nicholas R. Rodofile, Thomas Schmidt, Sebastian T. Sherry, Christopher Djamaludin, Kenneth Radke, and Ernest Foo</i>	
Solving the DLP with Low Hamming Weight Product Exponents and Improved Attacks on the GPS Identification Scheme.	460
<i>Jason H.M. Ying and Noboru Kunihiro</i>	
Author Index	469

Information Security and Privacy

22nd Australasian Conference, ACISP 2017, Auckland,
New Zealand, July 3-5, 2017, Proceedings, Part I

Pieprzyk, J.; Suriadi, S. (Eds.)

2017, XXIX, 471 p. 75 illus., Softcover

ISBN: 978-3-319-60054-3