

Contents

Post-quantum Cryptography

- On Quantum Related-Key Attacks on Iterated Even-Mansour Ciphers 3
Akinori Hosoyamada and Kazumaro Aoki
- The Beauty and the Beasts—The Hard Cases in LLL Reduction 19
Saed Alsayigh, Jintai Ding, Tsuyoshi Takagi, and Yuntao Wang

System Security (1)

- Simple Infeasibility Certificates for Attack Trees 39
Ahto Buldas, Aleksandr Lenin, Jan Willemsen, and Anton Charnamord
- Enhanced TLS Handshake Authentication with Blockchain and Smart Contract (Short Paper) 56
Bingqing Xia, Dongyao Ji, and Gang Yao

Public Key Cryptosystems (1)

- Multipurpose Public-Key Encryption 69
Rui Zhang and Kai He
- Secure Certificateless Proxy Re-encryption Without Pairing 85
Veronika Kuchta, Gaurav Sharma, Rajeev Anand Sahu, Tarunpreet Bhatia, and Olivier Markowitch

System Security (2)

- Not All Browsers are Created Equal: Comparing Web Browser Fingerprintability. 105
Nasser Mohammed Al-Fannah and Wanpeng Li
- Evasion Attacks Against Statistical Code Obfuscation Detectors 121
Jiawei Su, Danilo Vasconcellos Vargas, and Kouichi Sakurai

Cryptanalysis

- Analyzing Key Schedule of SIMON: Iterative Key Differences and Application to Related-Key Impossible Differentials 141
Kota Kondo, Yu Sasaki, Yosuke Todo, and Tetsu Iwata

Security Analysis of a Verifiable Server-Aided Approximate Similarity Computation 159
Rui Xu, Kirill Morozov, Anirban Basu, Mohammad Shahriar Rahman, and Shinsaku Kiyomoto

Cryptographic Protocols

Correction of a Secure Comparison Protocol for Encrypted Integers in IEEE WIFS 2012 (Short Paper). 181
Baptiste Vinh Mau and Koji Nuida

Adaptive Security in Identity-Based Authenticated Key Agreement with Multiple Private Key Generators 192
Atsushi Fujioka

Public Key Cryptosystems (2)

Deterministic Identity-Based Encryption from Lattices with More Compact Public Parameters 215
Daode Zhang, Fuyang Fang, Bao Li, and Xin Wang

IND-PCA Secure KEM Is Enough for Password-Based Authenticated Key Exchange (Short Paper) 231
Haiyang Xue, Bao Li, and Xianhui Lu

Author Index 243



<http://www.springer.com/978-3-319-64199-7>

Advances in Information and Computer Security
12th International Workshop on Security, IWSEC 2017,
Hiroshima, Japan, August 30 - September 1, 2017,
Proceedings
Obana, S.; Chida, K. (Eds.)
2017, XII, 243 p. 52 illus., Softcover
ISBN: 978-3-319-64199-7