Contents

RSA Security

General Bounds for Small Inverse Problems and Its Applications to Multi-Prime RSA ................................................. 3
Atsushi Takayasu and Noboru Kunihiro

On the Security of Distributed Multiprime RSA ......................... 18
Ivan Damgård, Gert Læsøe Mikkelsen, and Tue Skelved

Digital Signature

Formal Modeling of Random Oracle Programmability and Verification of Signature Unforgeability Using Task-PIOAs .............. 37
Kazuki Yoneyama

Algebraic Cryptanalysis of Yasuda, Takagi and Sakurai’s Signature Scheme . . . 53
Wenbin Zhang and Chik How Tan

Public Key Cryptography

Discrete Logarithms for Torsion Points on Elliptic Curve of Embedding Degree 1 ............................................................... 69
Yasuyuki Nogami and Hwajeong Seo

Efficient Key Dependent Message Security Amplification Against Chosen Ciphertext Attacks ............................................. 84
Fuyuki Kitagawa, Takahiro Matsuda, Goichiro Hanaoka, and Keisuke Tanaka

A Fast Phase-based Enumeration Algorithm for SVP Challenge Through $y$-Sparse Representations of Short Lattice Vectors .......... 101
Dan Ding, Guizhen Zhu, Yang Yu, and Zhongxiang Zheng

Block Ciphers

How Much Can Complexity of Linear Cryptanalysis Be Reduced? ........ 117
Sho Sakikoyama, Yosuke Todo, Kazumaro Aoki, and Masakatu Morii

Format-Preserving Encryption Algorithms Using Families of Tweakable Blockciphers ......................................................... 132
Jung-Keun Lee, Bonwook Koo, Dongyoung Roh, Woo-Hwan Kim, and Daesung Kwon
Bicliques with Minimal Data and Time Complexity for AES

Andrey Bogdanov, Donghoon Chang, Mohona Ghosh, and Somitra Kumar Sanadhya

Fault Analysis on SIMON Family of Lightweight Block Ciphers

Junko Takahashi and Toshinori Fukunaga

Network Security

A Clustering Approach for Privacy-Preserving in Social Networks

Rong Wang, Min Zhang, Dengguo Feng, and Yanyan Fu

Securely Solving Classical Network Flow Problems

Abdelrahaman Aly and Mathieu Van Vyve

Remote IP Protection Using Timing Channels

Ariano-Tim Donda, Peter Samarin, Jacek Samotyja, Kerstin Lemke-Rust, and Christof Paar

Mobile Security

Detecting Camouflaged Applications on Mobile Application Markets

Su Mon Kywe, Yingjiu Li, Robert H. Deng, and Jason Hong

WrapDroid: Flexible and Fine-Grained Scheme Towards Regulating Behaviors of Android Apps

Xueqiang Wang, Yuewu Wang, Limin Liu, Lingguang Lei, and Jiwu Jing

Hash Functions

A Collision Attack on a Double-Block-Length Compression Function Instantiated with Round-Reduced AES-256

Jiageng Chen, Shoichi Hirose, Hidenori Kuwakado, and Atsuko Miyaji

LSH: A New Fast Secure Hash Function Family

Dong-Chan Kim, Deukjo Hong, Jung-Keun Lee, Woo-Hwan Kim, and Daesung Kwon

Information Hiding and Efficiency

Lossless Data Hiding for Binary Document Images Using n-Pairs Pattern

Cheonshik Kim, Jinsuk Baek, and Paul S. Fisher

Montgomery Modular Multiplication on ARM-NEON Revisited

Hwajeong Seo, Zhe Liu, Johann Großschädl, Jongseok Choi, and Howon Kim
A Fair and Efficient Mutual Private Set Intersection Protocol from a Two-Way Oblivious Pseudorandom Function .......................... 343
   Sumit Kumar Debnath and Ratna Dutta

Cryptographic Protocol

Security Analysis of Polynomial Interpolation-Based Distributed Oblivious Transfer Protocols .................................................. 363
   Christian L.F. Corniaux and Hossein Ghodosi

Compact and Efficient UC Commitments Under Atomic-Exchanges ........... 381
   Ioana Boureanu and Serge Vaudenay

Issuer-Free Adaptive Oblivious Transfer with Access Policy .................. 402
   Vandana Guleria and Ratna Dutta

Side-Channel Attacks

Memory Address Side-Channel Analysis on Exponentiation .................... 421
   Chien-Ning Chen

Mutant Differential Fault Analysis of Trivium MDFA .......................... 433
   Mohamed Saied Emam Mohamed and Johannes Buchmann

Author Index .................................................................................. 447
Information Security and Cryptology – ICISC 2014
17th International Conference, Seoul, South Korea,
December 3–5, 2014, Revised Selected Papers
Lee, J.; Kim, J. (Eds.)
2015, XIII, 448 p. 83 illus., Softcover
ISBN: 978-3-319-15942-3