

Contents

RSA Security

General Bounds for Small Inverse Problems and Its Applications to Multi-Prime RSA	3
<i>Atsushi Takayasu and Noboru Kunihiro</i>	
On the Security of Distributed Multiprime RSA	18
<i>Ivan Damgård, Gert Læssøe Mikkelsen, and Tue Skeltved</i>	

Digital Signature

Formal Modeling of Random Oracle Programmability and Verification of Signature Unforgeability Using Task-PIOAs	37
<i>Kazuki Yoneyama</i>	
Algebraic Cryptanalysis of Yasuda, Takagi and Sakurai's Signature Scheme . . .	53
<i>Wenbin Zhang and Chik How Tan</i>	

Public Key Cryptography

Discrete Logarithms for Torsion Points on Elliptic Curve of Embedding Degree 1	69
<i>Yasuyuki Nogami and Hwajeong Seo</i>	
Efficient Key Dependent Message Security Amplification Against Chosen Ciphertext Attacks.	84
<i>Fuyuki Kitagawa, Takahiro Matsuda, Goichiro Hanaoka, and Keisuke Tanaka</i>	
A Fast Phase-based Enumeration Algorithm for SVP Challenge Through y -Sparse Representations of Short Lattice Vectors	101
<i>Dan Ding, Guizhen Zhu, Yang Yu, and Zhongxiang Zheng</i>	

Block Ciphers

How Much Can Complexity of Linear Cryptanalysis Be Reduced?	117
<i>Sho Sakikoyama, Yosuke Todo, Kazumaro Aoki, and Masakatu Morii</i>	
Format-Preserving Encryption Algorithms Using Families of Tweakable Blockciphers.	132
<i>Jung-Keun Lee, Bonwook Koo, Dongyoung Roh, Woo-Hwan Kim, and Daesung Kwon</i>	

Bicliques with Minimal Data and Time Complexity for AES	160
<i>Andrey Bogdanov, Donghoon Chang, Mohona Ghosh, and Somitra Kumar Sanadhya</i>	

Fault Analysis on SIMON Family of Lightweight Block Ciphers	175
<i>Junko Takahashi and Toshinori Fukunaga</i>	

Network Security

A Clustering Approach for Privacy-Preserving in Social Networks	193
<i>Rong Wang, Min Zhang, Dengguo Feng, and Yanyan Fu</i>	

Securely Solving Classical Network Flow Problems	205
<i>Abdelrahman Aly and Mathieu Van Vyve</i>	

Remote IP Protection Using Timing Channels	222
<i>Ariano-Tim Donda, Peter Samarin, Jacek Samotyja, Kerstin Lemke-Rust, and Christof Paar</i>	

Mobile Security

Detecting Camouflaged Applications on Mobile Application Markets	241
<i>Su Mon Kywe, Yingjiu Li, Robert H. Deng, and Jason Hong</i>	

WrapDroid: Flexible and Fine-Grained Scheme Towards Regulating Behaviors of Android Apps	255
<i>Xueqiang Wang, Yuewu Wang, Limin Liu, Lingguang Lei, and Jiwu Jing</i>	

Hash Functions

A Collision Attack on a Double-Block-Length Compression Function Instantiated with Round-Reduced AES-256	271
<i>Jiageng Chen, Shoichi Hirose, Hidenori Kuwakado, and Atsuko Miyaji</i>	

LSH: A New Fast Secure Hash Function Family.	286
<i>Dong-Chan Kim, Deukjo Hong, Jung-Keun Lee, Woo-Hwan Kim, and Daesung Kwon</i>	

Information Hiding and Efficiency

Lossless Data Hiding for Binary Document Images Using n -Pairs Pattern . . .	317
<i>Cheonshik Kim, Jinsuk Baek, and Paul S. Fisher</i>	

Montgomery Modular Multiplication on ARM-NEON Revisited	328
<i>Hwajeong Seo, Zhe Liu, Johann Großschädl, Jongseok Choi, and Howon Kim</i>	

A Fair and Efficient Mutual Private Set Intersection Protocol from a Two-Way Oblivious Pseudorandom Function	343
<i>Sumit Kumar Debnath and Ratna Dutta</i>	

Cryptographic Protocol

Security Analysis of Polynomial Interpolation-Based Distributed Oblivious Transfer Protocols	363
<i>Christian L.F. Corniaux and Hossein Ghodsi</i>	

Compact and Efficient UC Commitments Under Atomic-Exchanges	381
<i>Ioana Boureanu and Serge Vaudenay</i>	

Issuer-Free Adaptive Oblivious Transfer with Access Policy	402
<i>Vandana Guleria and Ratna Dutta</i>	

Side-Channel Attacks

Memory Address Side-Channel Analysis on Exponentiation	421
<i>Chien-Ning Chen</i>	

Mutant Differential Fault Analysis of Trivium MDFA	433
<i>Mohamed Saied Emam Mohamed and Johannes Buchmann</i>	

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