

Contents

Protocols

A Secure Group-Based AKA Protocol for Machine-Type Communications	3
<i>Rosario Giustolisi, Christian Gehrman, Markus Ahlström, and Simon Holmberg</i>	
Secure and Private, yet Lightweight, Authentication for the IoT via PUF and CBKA	28
<i>Christopher Huth, Aydin Aysu, Jorge Guajardo, Paul Duplys, and Tim Güneysu</i>	

Lattice Cryptography

A Practical Post-Quantum Public-Key Cryptosystem Based on spLWE	51
<i>Jung Hee Cheon, Kyoohyung Han, Jinsu Kim, Changmin Lee, and Yongha Son</i>	
Analysis of Error Terms of Signatures Based on Learning with Errors	75
<i>Jeongsu Kim, Suyong Park, Seonggeun Kim, Busik Jang, Sang Geun Hahn, Sangim Jung, and Dongyoung Roh</i>	

Encryption

Transforming Hidden Vector Encryption Schemes from Composite to Prime Order Groups	101
<i>Kwangsue Lee</i>	
Lossy Key Encapsulation Mechanism and Its Applications	126
<i>Yamin Liu, Xianhui Lu, Bao Li, and Haiyang Xue</i>	
Expanded Framework for Dual System Encryption and Its Application	145
<i>Minqian Wang and Zhenfeng Zhang</i>	
Adaptively Secure Broadcast Encryption with Dealership	161
<i>Kamalesh Acharya and Ratna Dutta</i>	

Implementation and Algorithms

A New Algorithm for Residue Multiplication Modulo $2^{521} - 1$	181
<i>Shoukat Ali and Murat Cenk</i>	

Enhancing Data Parallelism of Fully Homomorphic Encryption	194
<i>Paulo Martins and Leonel Sousa</i>	
An Improvement of Optimal Ate Pairing on KSS Curve with Pseudo 12-Sparse Multiplication	208
<i>Md. Al-Amin Khandaker, Hirotaka Ono, Yasuyuki Nogami, Masaaki Shirase, and Sylvain Duquesne</i>	
Signatures (and Protocol)	
Revisiting the Cubic UOV Signature Scheme	223
<i>Dung H. Duong, Albrecht Petzoldt, Yacheng Wang, and Tsuyoshi Takagi</i>	
Network Coding Signature Schemes Against Related-Key Attacks in the Random Oracle Model	239
<i>Jinyong Chang, Honglong Dai, Maozhi Xu, and Rui Xue</i>	
New Realizations of Efficient and Secure Private Set Intersection Protocols Preserving Fairness	254
<i>Sumit Kumar Debnath and Ratna Dutta</i>	
Analysis	
Improved Results on Cryptanalysis of Prime Power RSA	287
<i>Liqiang Peng, Lei Hu, and Yao Lu</i>	
On Computing the Immunity of Boolean Power Functions Against Fast Algebraic Attacks	304
<i>Yusong Du and Baodian Wei</i>	
Improved Fault Analysis on the Block Cipher SPECK by Injecting Faults in the Same Round	317
<i>Jingyi Feng, Hua Chen, Si Gao, Limin Fan, and Dengguo Feng</i>	
On the Effectiveness of Code-Reuse-Based Android Application Obfuscation.	333
<i>Xiaoxiao Tang, Yu Liang, Xinjie Ma, Yan Lin, and Debin Gao</i>	
Author Index	351

Information Security and Cryptology – ICISC 2016
19th International Conference, Seoul, South Korea,
November 30 – December 2, 2016, Revised Selected
Papers
Hong, S.; Park, J.H. (Eds.)
2017, XVI, 351 p. 31 illus., Softcover
ISBN: 978-3-319-53176-2