

# Contents

## Symmetric Ciphers

Biclique Attack of Block Cipher SKINNY . . . . .	3
<i>Yafei Zheng and Wenling Wu</i>	
Improved Differential Cryptanalysis of CAST-128 and CAST-256 . . . . .	18
<i>Shaomei Wang, Tingting Cui, and Meiqin Wang</i>	
Improved Integral and Zero-correlation Linear Cryptanalysis of CLEFIA Block Cipher. . . . .	33
<i>Wentan Yi, Baofeng Wu, Shaozhen Chen, and Dongdai Lin</i>	
Impossible Differentials of SPN Ciphers . . . . .	47
<i>Xuan Shen, Guoqiang Liu, Bing Sun, and Chao Li</i>	
SPF: A New Family of Efficient Format-Preserving Encryption Algorithms . . .	64
<i>Donghoon Chang, Mohona Ghosh, Kishan Chand Gupta, Arpan Jati, Abhishek Kumar, Dukjae Moon, Indranil Ghosh Ray, and Somitra Kumar Sanadhya</i>	
Transposition of AES Key Schedule . . . . .	84
<i>Jialin Huang, Hailun Yan, and Xuejia Lai</i>	
Revisiting the Security Proof of QUAD Stream Cipher: Some Corrections and Tighter Bounds. . . . .	103
<i>Goutam Paul and Abhiroop Sanyal</i>	

## Public-Key Cryptosystems

Achieving IND-CCA Security for Functional Encryption for Inner Products . . .	119
<i>Shiwei Zhang, Yi Mu, and Guomin Yang</i>	
An Improved Analysis on Three Variants of the RSA Cryptosystem . . . . .	140
<i>Liqiang Peng, Lei Hu, Yao Lu, and Hongyun Wei</i>	
How to Make the Cramer-Shoup Cryptosystem Secure Against Linear Related-Key Attacks . . . . .	150
<i>Baodong Qin, Shuai Han, Yu Chen, Shengli Liu, and Zhuo Wei</i>	

**Signature and Authentication**

On Privacy-Preserving Biometric Authentication . . . . .	169
<i>Aysajan Abidin</i>	
A Lightweight Authentication and Key Agreement Scheme for Mobile Satellite Communication Systems . . . . .	187
<i>Xinghua Wu, Aixin Zhang, Jianhua Li, Weiwei Zhao, and Yuchen Liu</i>	
Identity-Based Blind Signature from Lattices in Standard Model . . . . .	205
<i>Wen Gao, Yupu Hu, Baocang Wang, and Jia Xie</i>	

**Homomorphic Encryption**

Multi-bit Leveled Homomorphic Encryption via Dual.LWE-Based . . . . .	221
<i>Zengpeng Li, Chunguang Ma, Eduardo Morais, and Gang Du</i>	
Cryptanalysis of a Homomorphic Encryption Scheme Over Integers . . . . .	243
<i>Jingguo Bi, Jiayang Liu, and Xiaoyun Wang</i>	
Fully Homomorphic Encryption for Point Numbers . . . . .	253
<i>Seiko Arita and Shota Nakasato</i>	

**Leakage-Resilient**

Bounded-Retrieval Model with Keys Derived from Private Data . . . . .	273
<i>Konrad Durnoga, Stefan Dziembowski, Tomasz Kazana, Michał Zając, and Maciej Zdanowicz</i>	
Leakage-Resilient IND-CCA KEM from the Extractable Hash Proofs with Indistinguishability Obfuscation . . . . .	291
<i>Wenpan Jing, Xianhui Lu, and Bao Li</i>	
Codes for Detection of Limited View Algebraic Tampering . . . . .	309
<i>Fuchun Lin, Reihaneh Safavi-Naini, and Pengwei Wang</i>	

**Post-quantum Cryptography**

On Fast Calculation of Addition Chains for Isogeny-Based Cryptography . . .	323
<i>Brian Koziel, Reza Azarderakhsh, David Jao, and Mehran Mozaffari-Kermani</i>	
A Linear Algebra Attack on the Non-commuting Cryptography Class Based on Matrix Power Function . . . . .	343
<i>Jinhui Liu, Huanguo Zhang, and Jianwei Jia</i>	

**Commitment and Protocol**

Partial Bits Exposure Attacks on a New Commitment Scheme Based on the Zagier Polynomial. . . . .	357
<i>Xiaona Zhang and Li-Ping Wang</i>	
Key Predistribution Schemes Using Bent Functions in Distributed Sensor Networks. . . . .	367
<i>Deepak Kumar Dalai and Pinaki Sarkar</i>	
One-Round Cross-Domain Group Key Exchange Protocol in the Standard Model. . . . .	386
<i>Xiao Lan, Jing Xu, Hui Guo, and Zhenfeng Zhang</i>	

**Elliptic Curves**

On Constructing Parameterized Families of Pairing-Friendly Elliptic Curves with $\rho = 1$ . . . . .	403
<i>Meng Zhang, Zhi Hu, and Maozhi Xu</i>	
Constructing Isogenies on Extended Jacobi Quartic Curves . . . . .	416
<i>Xiu Xu, Wei Yu, Kunpeng Wang, and Xiaoyang He</i>	

**Security and Implementation**

Cyber-Attacks on Remote State Estimation in Industrial Control System: A Game-Based Framework. . . . .	431
<i>Cong Chen and Dongdai Lin</i>	
Secure Collaborative Outsourced k-Nearest Neighbor Classification with Multiple Owners in Cloud Environment . . . . .	451
<i>Hong Rong, Huimei Wang, Jian Liu, Wei Wu, Jialu Hao, and Ming Xian</i>	
Video Steganalysis Based on Centralized Error Detection in Spatial Domain. . .	472
<i>Yu Wang, Yun Cao, and Xianfeng Zhao</i>	
Log Your Car: Reliable Maintenance Services Record. . . . .	484
<i>Hafizah Mansor, Konstantinos Markantonakis, Raja Naeem Akram, Keith Mayes, and Iakovos Gurulian</i>	
Provably Secure Fair Mutual Private Set Intersection Cardinality Utilizing Bloom Filter . . . . .	505
<i>Sumit Kumar Debnath and Ratna Dutta</i>	
Evaluating Entropy for True Random Number Generators: Efficient, Robust and Provably Secure. . . . .	526
<i>Maciej Skorski</i>	
<b>Author Index</b> . . . . .	543

Information Security and Cryptology

12th International Conference, Inscrypt 2016, Beijing,  
China, November 4-6, 2016, Revised Selected Papers

Chen, K.; Lin, D.; Yung, M. (Eds.)

2017, XIII, 544 p. 78 illus., Softcover

ISBN: 978-3-319-54704-6