

# Contents

## Cryptanalysis

Truncated and Multiple Differential Cryptanalysis of Reduced Round Midori128 . . . . .	3
<i>Mohamed Tolba, Ahmed Abdelkhalik, and Amr M. Youssef</i>	
Improved Linear Cryptanalysis of Round-Reduced ARIA. . . . .	18
<i>Ahmed Abdelkhalik, Mohamed Tolba, and Amr M. Youssef</i>	
Partial Key Exposure Attacks on CRT-RSA: General Improvement for the Exposed Least Significant Bits . . . . .	35
<i>Atsushi Takayasu and Noboru Kunihiro</i>	
Cryptanalysis and Improved Construction of a Group Key Agreement for Secure Group Communication . . . . .	48
<i>Jun Xu, Lei Hu, Xiaona Zhang, Liqiang Peng, and Zhangjie Huang</i>	
Enhanced Correlation Power Analysis by Biasing Power Traces . . . . .	59
<i>Changhai Ou, Zhu Wang, Degang Sun, Xinpeng Zhou, Juan Ai, and Na Pang</i>	
Damaging, Simplifying, and Salvaging p-OMD . . . . .	73
<i>Tomer Ashur and Bart Mennink</i>	

## Cryptographic Protocols

Blind Password Registration for Two-Server Password Authenticated Key Exchange and Secret Sharing Protocols. . . . .	95
<i>Franziskus Kiefer and Mark Manulis</i>	
Chip Authentication for E-Passports: PACE with Chip Authentication Mapping v2 . . . . .	115
<i>Lucjan Hanzlik and Mirosław Kutylowski</i>	
AEP-M: Practical Anonymous E-Payment for Mobile Devices Using ARM TrustZone and Divisible E-Cash . . . . .	130
<i>Bo Yang, Kang Yang, Zhenfeng Zhang, Yu Qin, and Dengguo Feng</i>	
Universally Composable Two-Server PAKE. . . . .	147
<i>Franziskus Kiefer and Mark Manulis</i>	
Yet Another Note on Block Withholding Attack on Bitcoin Mining Pools . . .	167
<i>Samiran Bag and Kouichi Sakurai</i>	

**Network and Systems Security and Access Control**

Cyber Security Risk Assessment of a DDoS Attack. . . . . 183  
*Gaute Wangen, Andrii Shalaginov, and Christoffer Hallstensen*

Moving Target Defense Against Network Reconnaissance with Software  
Defined Networking . . . . . 203  
*Li Wang and Dinghao Wu*

Uni-ARBARC: A Unified Administrative Model for Role-Based  
Access Control . . . . . 218  
*Prosunjit Biswas, Ravi Sandhu, and Ram Krishnan*

SKALD: A Scalable Architecture for Feature Extraction, Multi-user  
Analysis, and Real-Time Information Sharing. . . . . 231  
*George D. Webster, Zachary D. Hanif, Andre L.P. Ludwig,  
Tamas K. Lengyel, Apostolis Zarras, and Claudia Eckert*

**Privacy and Watermarking**

Leveraging Internet Services to Evade Censorship. . . . . 253  
*Apostolis Zarras*

Analyzing Randomized Response Mechanisms Under Differential Privacy . . . 271  
*Atsushi Waseda and Ryo Nojima*

Models and Algorithms for Graph Watermarking . . . . . 283  
*David Eppstein, Michael T. Goodrich, Jenny Lam, Nil Mamano,  
Michael Mitzenmacher, and Manuel Torres*

**Software Security**

Policy-Based Implicit Attestation for Microkernel-Based  
Virtualized Systems. . . . . 305  
*Steffen Wagner and Claudia Eckert*

Generalized Dynamic Opaque Predicates: A New Control Flow  
Obfuscation Method . . . . . 323  
*Dongpeng Xu, Jiang Ming, and Dinghao Wu*

A Bayesian Cognitive Approach to Quantifying Software Exploitability  
Based on Reachability Testing . . . . . 343  
*Guanhua Yan, Yunus Kucuk, Max Slocum, and David C. Last*

Control Flow Integrity Enforcement with Dynamic Code Optimization . . . . . 366  
*Yan Lin, Xiaoxiao Tang, Debin Gao, and Jianming Fu*

**Encryption, Signatures and Fundamentals**

Impossibility on the Provable Security of the Fiat-Shamir-Type Signatures  
in the Non-programmable Random Oracle Model . . . . . 389  
*Masayuki Fukumitsu and Shingo Hasegawa*

Efficient Functional Encryption for Inner-Product Values  
with Full-Hiding Security. . . . . 408  
*Junichi Tomida, Masayuki Abe, and Tatsuaki Okamoto*

MQSAS - A Multivariate Sequential Aggregate Signature Scheme . . . . . 426  
*Rachid El Bansarkhani, Mohamed Saied Emam Mohamed,  
and Albrecht Petzoldt*

Cryptanalysis of Multi-Prime  $\Phi$ -Hiding Assumption . . . . . 440  
*Jun Xu, Lei Hu, Santanu Sarkar, Xiaona Zhang, Zhangjie Huang,  
and Liqiang Peng*

**Author Index** . . . . . 455



<http://www.springer.com/978-3-319-45870-0>

Information Security

19th International Conference, ISC 2016, Honolulu, HI,

USA, September 3-6, 2016. Proceedings

Bishop, M.; Nascimento, A.C.A. (Eds.)

2016, XIII, 455 p. 92 illus., Softcover

ISBN: 978-3-319-45870-0