Contents

Hash Function

Biclique Cryptanalysis of Full Round AES-128 Based Hashing Modes . . . . . . . . . . 3  
Donghoon Chang, Mohona Ghosh, and Somitra Kumar Sanadhya

Hashing into Generalized Huff Curves . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 22  
Xiaoyang He, Wei Yu, and Kunpeng Wang

Signature Schemes

Cubic Unbalance Oil and Vinegar Signature Scheme . . . . . . . . . . . . . . . . . . . . . 47  
Xuyun Nie, Bo Liu, Hu Xiong, and Gang Lu

Two Approaches to Build UOV Variants with Shorter Private Key  
and Faster Signature Generation . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 57  
Yang Tan and Shaohua Tang

A Secure Variant of Yasuda, Takagi and Sakurai’s Signature Scheme . . . . . . . . . . 75  
Wenbin Zhang and Chik How Tan

Symmetric Ciphers

Statistical and Algebraic Properties of DES . . . . . . . . . . . . . . . . . . . . . . . . . . . 93  
Stian Fauskanger and Igor Semaev

Accurate Estimation of the Full Differential Distribution for General  
Feistel Structures . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 108  
Jiageng Chen, Atsuko Miyaji, Chunhua Su, and Je Sen Teh

Improved Zero-Correlation Cryptanalysis on SIMON . . . . . . . . . . . . . . . . . . . . 125  
Ling Sun, Kai Fu, and Meiqin Wang

A New Cryptographic Analysis of 4-bit S-Boxes . . . . . . . . . . . . . . . . . . . . . . . 144  
Ling Cheng, Wentao Zhang, and Zejun Xiang

Elliptic Curve and Cryptographic Fundamentals

On Generating Coset Representatives of PGL2(Fq) in PGL2(Fq2) . . . . . . . . . . . . 167  
Jincheng Zhuang and Qi Cheng

Recovering a Sum of Two Squares Decomposition Revisited . . . . . . . . . . . . . . . 178  
Xiaona Zhang, Li-Ping Wang, Jun Xu, Lei Hu, Liqiang Peng,  
Zhangjie Huang, and Zeyi Liu
Improved Tripling on Elliptic Curves. ........................................ 193
Weixuan Li, Wei Yu, and Kunpeng Wang

Web and Application Security

An Approach for Mitigating Potential Threats in Practical SSO Systems .... 209
Menghao Li, Liang Yang, Zimu Yuan, Rui Zhang, and Rui Xue

EQPO: Obscuring Encrypted Web Traffic with Equal-Sized
Pseudo-Objects ................................................................. 227
Yi Tang and Manjia Lin

A Blind Dual Color Images Watermarking Method via SVD
and DNA Sequences ............................................................ 246
Xiangjun Wu and Haibin Kan

On the Application of Clique Problem for Proof-of-Work
in Cryptocurrencies ............................................................. 260
Samiran Bag, Sushmita Ruj, and Kouichi Sakurai

Cloud Security

Proxy Provable Data Possession with General Access Structure
in Public Clouds ................................................................. 283
Huaqun Wang and Debiao He

A Provable Data Possession Scheme with Data Hierarchy in Cloud. ......... 301
Changlu Lin, Fucai Luo, Huaxiong Wang, and Yan Zhu

Threshold Broadcast Encryption with Keyword Search ....................... 322
Shiwei Zhang, Yi Mu, and Guomin Yang

Key Management and Public Key Encryption

Secret Sharing Schemes with General Access Structures ....................... 341
Jian Liu, Sihem Mesnager, and Lusheng Chen

CCA Secure Public Key Encryption Scheme Based on LWE Without
Gaussian Sampling ............................................................ 361
Xiaochao Sun, Bao Li, Xianhui Lu, and Fuyang Fang

Zero Knowledge and Secure Computations

Slow Motion Zero Knowledge Identifying with Colliding Commitments .... 381
Houda Ferradi, Rémi Géraud, and David Naccache
Multi-client Outsourced Computation. ......................... 397
   Peili Li, Haixia Xu, and Yuanyuan Ji

Software and Mobile Security

Privacy-Enhanced Data Collection Scheme for Smart-Metering. .......... 413
   Jan Hajny, Petr Dzurenda, and Lukas Malina

A Secure Architecture for Operating System-Level Virtualization
on Mobile Devices .............................................. 430
   Manuel Huber, Julian Horsch, Michael Velten, Michael Weiss,
   and Sascha Wessel

Assessing the Disclosure of User Profile in Mobile-Aware Services. .... 451
   Daiyong Quan, Lihuan Yin, and Yunchuan Guo

Interactive Function Identification Decreasing the Effort of Reverse
Engineering ....................................................... 468
   Fatih Kilic, Hannes Laner, and Claudia Eckert

Author Index ....................................................... 489
Information Security and Cryptology
11th International Conference, Inscrypt 2015, Beijing, China, November 1-3, 2015, Revised Selected Papers
Lin, D.; Wang, X.; Yung, M. (Eds.)
2016, XIV, 490 p. 102 illus., Softcover
ISBN: 978-3-319-38897-7