

Contents

Hash Function

Biclique Cryptanalysis of Full Round AES-128 Based Hashing Modes	3
<i>Donghoon Chang, Mohona Ghosh, and Somitra Kumar Sanadhya</i>	
Hashing into Generalized Huff Curves.	22
<i>Xiaoyang He, Wei Yu, and Kunpeng Wang</i>	

Signature Schemes

Cubic Unbalance Oil and Vinegar Signature Scheme.	47
<i>Xuyun Nie, Bo Liu, Hu Xiong, and Gang Lu</i>	
Two Approaches to Build UOV Variants with Shorter Private Key and Faster Signature Generation	57
<i>Yang Tan and Shaohua Tang</i>	
A Secure Variant of Yasuda, Takagi and Sakurai's Signature Scheme	75
<i>Wenbin Zhang and Chik How Tan</i>	

Symmetric Ciphers

Statistical and Algebraic Properties of DES	93
<i>Stian Fauskanger and Igor Semaev</i>	
Accurate Estimation of the Full Differential Distribution for General Feistel Structures.	108
<i>Jiageng Chen, Atsuko Miyaji, Chunhua Su, and Je Sen Teh</i>	
Improved Zero-Correlation Cryptanalysis on SIMON.	125
<i>Ling Sun, Kai Fu, and Meiqin Wang</i>	
A New Cryptographic Analysis of 4-bit S-Boxes	144
<i>Ling Cheng, Wentao Zhang, and Zejun Xiang</i>	

Elliptic Curve and Cryptographic Fundamentals

On Generating Coset Representatives of $PGL_2(\mathbb{F}_q)$ in $PGL_2(\mathbb{F}_{q^2})$	167
<i>Jincheng Zhuang and Qi Cheng</i>	
Recovering a Sum of Two Squares Decomposition Revisited	178
<i>Xiaona Zhang, Li-Ping Wang, Jun Xu, Lei Hu, Liqiang Peng, Zhangjie Huang, and Zeyi Liu</i>	

Improved Tripling on Elliptic Curves.	193
<i>Weixuan Li, Wei Yu, and Kunpeng Wang</i>	

Web and Application Security

An Approach for Mitigating Potential Threats in Practical SSO Systems	209
<i>Menghao Li, Liang Yang, Zimu Yuan, Rui Zhang, and Rui Xue</i>	
EQPO: Obscuring Encrypted Web Traffic with Equal-Sized Pseudo-Objects	227
<i>Yi Tang and Manjia Lin</i>	
A Blind Dual Color Images Watermarking Method via SVD and DNA Sequences	246
<i>Xiangjun Wu and Haibin Kan</i>	
On the Application of Clique Problem for Proof-of-Work in Cryptocurrencies	260
<i>Samiran Bag, Sushmita Ruj, and Kouichi Sakurai</i>	

Cloud Security

Proxy Provable Data Possession with General Access Structure in Public Clouds	283
<i>Huaqun Wang and Debiao He</i>	
A Provable Data Possession Scheme with Data Hierarchy in Cloud.	301
<i>Changlu Lin, Fucui Luo, Huaxiong Wang, and Yan Zhu</i>	
Threshold Broadcast Encryption with Keyword Search	322
<i>Shiwei Zhang, Yi Mu, and Guomin Yang</i>	

Key Management and Public Key Encryption

Secret Sharing Schemes with General Access Structures	341
<i>Jian Liu, Sihem Mesnager, and Lusheng Chen</i>	
CCA Secure Public Key Encryption Scheme Based on LWE Without Gaussian Sampling	361
<i>Xiaochao Sun, Bao Li, Xianhui Lu, and Fuyang Fang</i>	

Zero Knowledge and Secure Computations

Slow Motion Zero Knowledge Identifying with Colliding Commitments	381
<i>Houda Ferradi, Rémi Géraud, and David Naccache</i>	

Multi-client Outsourced Computation.	397
<i>Peili Li, Haixia Xu, and Yuanyuan Ji</i>	
Software and Mobile Security	
Privacy-Enhanced Data Collection Scheme for Smart-Metering.	413
<i>Jan Hajny, Petr Dzurenda, and Lukas Malina</i>	
A Secure Architecture for Operating System-Level Virtualization on Mobile Devices	430
<i>Manuel Huber, Julian Horsch, Michael Velten, Michael Weiss, and Sascha Wessel</i>	
Assessing the Disclosure of User Profile in Mobile-Aware Services.	451
<i>Daiyong Quan, Lihuan Yin, and Yunchuan Guo</i>	
Interactive Function Identification Decreasing the Effort of Reverse Engineering	468
<i>Fatih Kilic, Hannes Laner, and Claudia Eckert</i>	
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