

Contents

Boolean Function and Block Cipher

A Note on Semi-bent and Hyper-bent Boolean Functions	3
<i>Chunming Tang, Yu Lou, Yanfeng Qi, Maozhi Xu, and Baoan Guo</i>	
New Construction of Differentially 4-Uniform Bijections	22
<i>Claude Carlet, Deng Tang, Xiaohu Tang, and Qunying Liao</i>	
Automatic Security Evaluation of Block Ciphers with S-bP Structures Against Related-Key Differential Attacks	39
<i>Siwei Sun, Lei Hu, Ling Song, Yonghong Xie, and Peng Wang</i>	

Sequence and Stream Cipher

On the Key-Stream Periods Probability of Edon80	55
<i>Yunqing Xu</i>	
Cube Theory and Stable k -Error Linear Complexity for Periodic Sequences . . .	70
<i>Jianqin Zhou, Wanquan Liu, and Guanglu Zhou</i>	
Autocorrelation Values of New Generalized Cyclotomic Sequences of Order Six Over \mathbb{Z}_{pq}	86
<i>Xinxin Gong, Bin Zhang, Dengguo Feng, and Tongjiang Yan</i>	

Applications: Systems and Theory

Automatic Detection and Analysis of Encrypted Messages in Malware	101
<i>Ruoxu Zhao, Dawu Gu, Juanru Li, and Yuanyuan Zhang</i>	
EAdroid: Providing Environment Adaptive Security for Android System	118
<i>Hongliang Liang, Yu Dong, Bin Wang, and Shuchang Liu</i>	
Supervised Usage of Signature Creation Devices.	132
<i>Przemysław Kubiak and Mirosław Kutylowski</i>	
A Practical Attack on <i>Patched</i> MIFARE Classic	150
<i>Yi-Hao Chiu, Wei-Chih Hong, Li-Ping Chou, Jintai Ding, Bo-Yin Yang, and Chen-Mou Cheng</i>	

Computational Number Theory

Omega Pairing on Hyperelliptic Curves	167
<i>Shan Chen, Kunpeng Wang, Dongdai Lin, and Tao Wang</i>	
Pairing Computation on Edwards Curves with High-Degree Twists	185
<i>Liangze Li, Hongfeng Wu, and Fan Zhang</i>	
The Gallant-Lambert-Vanstone Decomposition Revisited	201
<i>Zhi Hu and Maozhi Xu</i>	
Low-Weight Primes for Lightweight Elliptic Curve Cryptography on 8-bit AVR Processors	217
<i>Zhe Liu, Johann Großschädl, and Duncan S. Wong</i>	

Public Key Cryptography

Secure One-to-Group Communications Escrow-Free ID-Based Asymmetric Group Key Agreement.	239
<i>Lei Zhang, Qianhong Wu, Josep Domingo-Ferrer, Bo Qin, Sherman S.M. Chow, and Wenchang Shi</i>	
Security Model and Analysis of FHMVQ, Revisited	255
<i>Shengli Liu, Kouichi Sakurai, Jian Weng, Fangguo Zhang, and Yunlei Zhao</i>	
RSA-OAEP Is RKA Secure	270
<i>Dingding Jia, Bao Li, Xianhui Lu, and Yamin Liu</i>	
A Note on a Signature Building Block and Relevant Security Reduction in the Green-Hohenberger OT Scheme.	282
<i>Zhengjun Cao, Frederic Lafitte, and Olivier Markowitch</i>	

Hash Function

LHash: A Lightweight Hash Function	291
<i>Wenling Wu, Shuang Wu, Lei Zhang, Jian Zou, and Le Dong</i>	
Cryptanalysis of the Round-Reduced GOST Hash Function	309
<i>Jian Zou, Wenling Wu, and Shuang Wu</i>	

Side-Channel and Leakage

Multivariate Leakage Model for Improving Non-profiling DPA on Noisy Power Traces	325
<i>Suvadeep Hajra and Debdeep Mukhopadhyay</i>	

Partially Known Nonces and Fault Injection Attacks on SM2 Signature Algorithm	343
<i>Mingjie Liu, Jiazhe Chen, and Hexin Li</i>	

Application and System Security

Environment-Bound SAML Assertions: A Fresh Approach to Enhance the Security of SAML Assertions	361
<i>Kai Chen, Dongdai Lin, Li Yan, and Xin Sun</i>	
One-Time Programs with Limited Memory	377
<i>Konrad Durnoga, Stefan Dziembowski, Tomasz Kazana, and Michal Zajac</i>	
Cryptanalysis of Three Authenticated Encryption Schemes for Wireless Sensor Networks	395
<i>Xiaoqian Li, Peng Wang, Bao Li, and Zhelei Sun</i>	
Author Index	407

Information Security and Cryptology

9th International Conference, Inscrypt 2013,

Guangzhou, China, November 27-30, 2013, Revised

Selected Papers

Lin, D.; Xu, S.; Yung, M. (Eds.)

2014, XIII, 408 p. 51 illus., Softcover

ISBN: 978-3-319-12086-7