Contents

Boolean Function and Block Cipher

A Note on Semi-bent and Hyper-bent Boolean Functions. . . . . . . . . . . . . . . 3
  Chunming Tang, Yu Lou, Yanfeng Qi, Maozhi Xu, and Baoan Guo

New Construction of Differentially 4-Uniform Bijections . . . . . . . . . . . . . . 22
  Claude Carlet, Deng Tang, Xiaohu Tang, and Qunying Liao

Automatic Security Evaluation of Block Ciphers with S-bP Structures
Against Related-Key Differential Attacks . . . . . . . . . . . . . . . . . . . . . . . . . . 39
  Siwei Sun, Lei Hu, Ling Song, Yonghong Xie, and Peng Wang

Sequence and Stream Cipher

On the Key-Stream Periods Probability of Edon80 . . . . . . . . . . . . . . . . . . . 55
  Yunqing Xu

Cube Theory and Stable k-Error Linear Complexity for Periodic Sequences . . . . 70
  Jianqin Zhou, Wanquan Liu, and Guanglu Zhou

Autocorrelation Values of New Generalized Cyclotomic Sequences
of Order Six Over $\mathbb{Z}_{pq}$ . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 86
  Xinxin Gong, Bin Zhang, Dengguo Feng, and Tongjiang Yan

Applications: Systems and Theory

Automatic Detection and Analysis of Encrypted Messages in Malware . . . . . . 101
  Ruoxu Zhao, Dawu Gu, Juanru Li, and Yuanyuan Zhang

EAdroid: Providing Environment Adaptive Security for Android System . . . . 118
  Hongliang Liang, Yu Dong, Bin Wang, and Shuchang Liu

Supervised Usage of Signature Creation Devices . . . . . . . . . . . . . . . . . . . 132
  Przemysław Kubiak and Mirosław Kutyłowski

A Practical Attack on Patched MIFARE Classic . . . . . . . . . . . . . . . . . . . 150
  Yi-Hao Chiu, Wei-Chih Hong, Li-Ping Chou, Jintai Ding, Bo-Yin Yang,
  and Chen-Mou Cheng
Computational Number Theory

Omega Pairing on Hyperelliptic Curves .................................................. 167
Shan Chen, Kunpeng Wang, Dongdai Lin, and Tao Wang

Pairing Computation on Edwards Curves with High-Degree Twists .......... 185
Liangze Li, Hongfeng Wu, and Fan Zhang

The Gallant-Lambert-Vanstone Decomposition Revisited ...................... 201
Zhi Hu and Maozhi Xu

Low-Weight Primes for Lightweight Elliptic Curve Cryptography
on 8-bit AVR Processors ................................................................. 217
Zhe Liu, Johann Großschädl, and Duncan S. Wong

Public Key Cryptography

Secure One-to-Group Communications Escrow-Free ID-Based
Asymmetric Group Key Agreement .................................................. 239
Lei Zhang, Qianhong Wu, Josep Domingo-Ferrer, Bo Qin,
Sherman S.M. Chow, and Wenchang Shi

Security Model and Analysis of FHMKV, Revisited ......................... 255
Shengli Liu, Kouichi Sakurai, Jian Weng, Fangguo Zhang, and Yunlei Zhao

RSA-OAEP Is RKA Secure ................................................................. 270
Dingding Jia, Bao Li, Xianhui Lu, and Yamin Liu

A Note on a Signature Building Block and Relevant Security Reduction
in the Green-Hohenberger OT Scheme .............................................. 282
Zhengjun Cao, Frederic Lafitte, and Olivier Markowitch

Hash Function

LHash: A Lightweight Hash Function .................................................. 291
Wenling Wu, Shuang Wu, Lei Zhang, Jian Zou, and Le Dong

Cryptanalysis of the Round-Reduced GOST Hash Function .................. 309
Jian Zou, Wenling Wu, and Shuang Wu

Side-Channel and Leakage

Multivariate Leakage Model for Improving Non-profiling DPA
on Noisy Power Traces ................................................................. 325
Suvadeep Hajra and Debdeep Mukhopadhyay
Partially Known Nonces and Fault Injection Attacks on SM2 Signature

Mingjie Liu, Jiazhe Chen, and Hexin Li

Application and System Security

Environment-Bound SAML Assertions: A Fresh Approach to Enhance the Security of SAML Assertions

Kai Chen, Dongdai Lin, Li Yan, and Xin Sun

One-Time Programs with Limited Memory

Konrad Durnoga, Stefan Dziembowski, Tomasz Kazana, and Michal Zając

Cryptanalysis of Three Authenticated Encryption Schemes for Wireless Sensor Networks

Xiaoqian Li, Peng Wang, Bao Li, and Zhelei Sun

Author Index
Information Security and Cryptology
9th International Conference, Inscrypt 2013,
Guangzhou, China, November 27-30, 2013, Revised
Selected Papers
Lin, D.; Xu, S.; Young, M. (Eds.)
2014, XIII, 408 p. 51 illus., Softcover
ISBN: 978-3-319-12086-7