Table of Contents

Full Papers

Applied Cryptography

Audio Steganalysis Based on Lossless Data-Compression Techniques 1
Fatiha Djebbar and Beghdad Ayad

Enhancing the Perceived Visual Quality of a Size Invariant Visual Cryptography Scheme 10
Yang-Wai Chow, Willy Susilo, and Duncan S. Wong

Impact of the Revocation Service in PKI Prices 22
Carlos Gañán, Jose L. Muñoz, Oscar Esparza, Jorge Mata-Díaz, and Juanjo Alins

Cryptanalysis

Cryptanalysis of Multi-Prime RSA with Small Prime Difference 33
Hatem M. Bahig, Ashraf Bhery, and Dieaa I. Nassr

Implicit Polynomial Recovery and Cryptanalysis of a Combinatorial Key Cryptosystem 45
Jun Xu, Lei Hu, and Siwei Sun

Improved Related-Key Differential Attacks on Reduced-Round LBlock 58
Shusheng Liu, Zheng Gong, and Libin Wang

Network Security

Countermeasures on Application Level Low-Rate Denial-of-Service Attack 70
Yajuan Tang

Firewall Packet Filtering Optimization Using Statistical Traffic Awareness Test 81
Zouheir Trabelsi, Liren Zhang, and Safaa Zeidan

Group Behavior Metrics for P2P Botnet Detection 93
John Felix, Charles Joseph, and Ali A. Ghorbani

Bibliografische Informationen
http://d-nb.info/1025944763

digitalisiert durch DEUTSCHE NATIONAL BIBLIOTHEK

Optimization

Hardware Performance Optimization and Evaluation of SM3 Hash Algorithm on FPGA 105
Yuan Ma, Luning Xia, Jingqiang Lin, Jiwu Jing, Zongbin Liu, and Xingjie Yu

Privacy

Continual Leakage-Resilient Dynamic Secret Sharing in the Split-State Model 119
Hao Xiong, Cong Zhang, Tsz Hon Yuen, Echo P. Zhang, Siu Ming Yiu, and Sihan Qing

Conversion of Real-Numbered Privacy-Preserving Problems into the Integer Domain 131
Wilko Henecka, Nigel Bean, and Matthew Roughan

Perfect Ambiguous Optimistic Fair Exchange 142
Yang Wang, Man Ho Au, and Willy Susilo

Privacy-Preserving Noisy Keyword Search in Cloud Computing 154
Xiaoqiong Pang, Bo Yang, and Qiong Huang

Protocols

Forward Secure Attribute-Based Signatures 167
Tsz Hon Yuen, Joseph K. Liu, Xinyi Huang, Man Ho Au, Willy Susilo, and Jianying Zhou

On Constant-Round Precise Zero-Knowledge 178
Ning Ding and Dawu Gu

Outsourcing Encryption of Attribute-Based Encryption with MapReduce 191
Jingwei Li, Chunfu Jia, Jin Li, and Xiaofeng Chen

Security Enhancement of Identity-Based Identification with Reversibility 202
Atsushi Fujioka, Taiichi Saito, and Keita Xagawa

Security in Mobile Systems

Coopetitive Architecture to Support a Dynamic and Scalable NFC Based Mobile Services Architecture 214
Raja Naeem Akram, Konstantinos Markantonakis, and Keith Mayes

Permission-Based Abnormal Application Detection for Android 228
Jiawei Zhu, Zhi Guan, Yang Yang, Liangwen Yu, Huiping Sun, and Zhong Chen

Symbian Smartphone Forensics and Security: Recovery of Privacy-Protected Deleted Data 240
Vrizlynn L.L. Thing and Darell J.J. Tan

Software Security

Detecting Encryption Functions via Process Emulation and IL-Based Program Analysis 252
Ruoxu Zhao, Dawu Gu, Juanru Li, and Hui Liu

Taint Analysis of Security Code in the KLEE Symbolic Execution Engine 264
Ricardo Corin and Felipe Andrés Manzano

Short Papers

Authentication

A Generic Approach for Providing Revocation Support in Secret Handshake 276
Yanjiang Yang, Haibing Lu, Jian Weng, Xuhua Ding, and Jianying Zhou

An Efficient Single-Slow-Phase Mutually Authenticated RFID Distance Bounding Protocol with Tag Privacy 285
Anjia Yang, Yunhui Zhuang, and Duncan S. Wong

Exploring Mobile Proxies for Better Password Authentication 293
Nitesh Saxena and Jonathan Voris

On Security of Universal Hash Function Based Multiple Authentication 303
Aysajan Abidin

Cryptanalysis

A New Variant of Time Memory Trade-Off on the Improvement of Thing and Ying's Attack 311
Zhenqi Li, Yao Lu, Wenhao Wang, Bin Zhang, and Dongdai Lin

Applying Time-Memory-Data Trade-Off to Plaintext Recovery Attack... 321
Zhenqi Li, Bin Zhang, Yao Lu, Jing Zou, and Dongdai Lin

Comparison between Side-Channel Analysis Distinguishers 331
Houssem Maghrebi, Olivier Rioul, Sylvain Guilley, and Jean-Luc Danger

Multimedia Security and GPU-Enabled Computation

Acceleration of Composite Order Bilinear Pairing on Graphics Hardware 341
Ye Zhang, Chun Jason Xue, Duncan S. Wong, Nikos Mamoulis, and Siu Ming Yiu

Evaluating the Effect of Tolerance on Click-Draw Based Graphical Password Scheme 349
Yuxin Meng and Wenjuan Li

Robust Evidence Detection of Copy-Rotate-Move Forgery in Image Based on Singular Value Decomposition 357
Liu Yong, Huang Meishan, and Lin Bogang

Network Security

Cookie-Proxy: A Scheme to Prevent SSLStrip Attack 365
Sendong Zhao, Ding Wang, Sicheng Zhao, Wu Yang, and Chunguang Ma

Detecting and Preventing ActiveX API-Misuse Vulnerabilities in Internet Explorer 373
Ting Dai, Sai Sathyanarayan, Roland H.C. Yap, and Zhenkai Liang

Endpoint Mitigation of DDoS Attacks Based on Dynamic Thresholding 381
Daewon Kim, Byoungkoo Kim, Ikkyun Kim, Jeongnyeo Kim, and Hyunsook Cho

Parameter Pollution Vulnerabilities Detection Study Based on Tree Edit Distance 392
Yan Cao, Qiang Wei, and Qingxian Wang

Privacy

A Privacy-Preserving Path-Checking Solution for RFID-Based Supply Chains 400
Wei Xin, Huiping Sun, Tao Yang, Zhi Guan, and Zhong Chen

Efficient Attribute Proofs in Anonymous Credential Using Attribute-Based Cryptography 408
Yan Zhang and Dengguo Feng

F^5P^5: Keyword Search over Encrypted Data with Five Functions and Five Privacy Assurances 416
Huimin Shuai and Wen Tao Zhu

Location Privacy Policy Management System 427
Arej Muhammed, Dan Lin, and Anna Squicciarini

Privacy Protection in Social Networks Using l-Diversity 435
Liangwen Yu, Jiawei Zhu, Zhengang Wu, Tao Yang, Jianbin Hu, and Zhong Chen

Selling Power Back to the Grid in a Secure and Privacy-Preserving Manner 445
Tat Wing Chim, Siu Ming Yiu, Lucas Chi Kwong Hui, Victor On Kwok Li, Tin Wing Mui, Yu Hin Tsang, Chun Kin Kwok, and Kwun Yin Yu

Protocols

A Key Sharing Fuzzy Vault Scheme 453
Lin You, Mengsheng Fan, Jie Lu, Shengguo Wang, and Fenghai Li

A New Version of McEliece PKC Based on Convolutional Codes 461
Carl Löndahl and Thomas Johansson

Flexible Attribute-Based Encryption 471
Seiko Arita

Non-interactive Dynamic Identity-Based Broadcast Encryption without Random Oracles 479
Yanli Ren, Shuozhong Wang, and Xinpeng Zhang

Software Security

A Comparative Study of Malware Family Classification 488
Rafiqul Islam and Irfan Altas

A Fine-Grained Classification Approach for the Packed Malicious Code 497
Shanqing Guo, Shuangshuang Li, Yan Yu, Anlei Hu, and Tao Ban

Author Index 505