

Contents

System Security

Operating System Security Policy Hardening via Capability Dependency Graphs	3
<i>Zhihui Han, Liang Cheng, Yang Zhang, and Dengguo Feng</i>	
Expanding an Operating System's Working Space with a New Mode to Support Trust Measurement	18
<i>Chenglong Wei, Wenchang Shi, Bo Qin, and Bin Liang</i>	

Stream Cipher I

Differential Fault Analysis of Streebog	35
<i>Riham AlTawy and Amr M. Youssef</i>	
Fault Attacks on Stream Cipher Scream	50
<i>Shaoyu Du, Bin Zhang, Zhenqi Li, and Dongdai Lin</i>	
New Related Key Attacks on the RAKAPOSHI Stream Cipher	65
<i>Lin Ding, Chenhui Jin, Jie Guan, Shaowu Zhang, Ting Cui, and Wei Zhao</i>	

Analysis

Cramer-Shoup Like Chosen Ciphertext Security from LPN	79
<i>Xiaochao Sun, Bao Li, and Xianhui Lu</i>	
Partial Prime Factor Exposure Attacks on RSA and Its Takagi's Variant	96
<i>Liqiang Peng, Lei Hu, Zhangjie Huang, and Jun Xu</i>	
Analysis of Fractional ω mbNAF for Scalar Multiplication	109
<i>Weixuan Li, Wei Yu, and Kunpeng Wang</i>	
On the Effectiveness of Different Botnet Detection Approaches.....	121
<i>Fariba Haddadi, Duc Le Cong, Laura Porter, and A. Nur Zincir-Heywood</i>	

Key Exchange Protocol

Strongly Secure Key Exchange Protocol with Minimal KEM.....	139
<i>Baoping Tian, Fushan Wei, and Chuangui Ma</i>	

sHMQV: An Efficient Key Exchange Protocol for Power-Limited
Devices 154
Shijun Zhao and Qianying Zhang

Elliptic Curve Cryptography

Models of Curves from GHS Attack in Odd Characteristic 171
Song Tian, Wei Yu, Bao Li, and Kunpeng Wang

Some Elliptic Subcovers of Genus 3 Hyperelliptic Curves 181
Song Tian, Wei Yu, Bao Li, and Kunpeng Wang

Batch Blind Signatures on Elliptic Curves 192
Yang Sun, Qianhong Wu, Bo Qin, Yujue Wang, and Jianwei Liu

Stream Cipher II

Improved Differential Analysis of Block Cipher PRIDE 209
*Qianqian Yang, Lei Hu, Siwei Sun, Kexin Qiao, Ling Song,
Jinyong Shan, and Xiaoshuang Ma*

Estimating Differential-Linear Distinguishers and Applications
to CTC2 220
Chun Guo, Hailong Zhang, and Dongdai Lin

Combined Cache Timing Attacks and Template Attacks on Stream
Cipher MUGI 235
Shaoyu Du, Zhenqi Li, Bin Zhang, and Dongdai Lin

Authentication

Half a Century of Practice: Who Is Still Storing Plaintext
Passwords? 253
Erick Bauman, Yafeng Lu, and Zhiqiang Lin

User Identity Verification Based on Touchscreen Interaction Analysis
in Web Contexts 268
Michael Velten, Peter Schneider, Sascha Wessel, and Claudia Eckert

Adaptive-ID Secure Revocable Identity-Based Encryption from Lattices
via Subset Difference Method 283
Shantian Cheng and Juanyang Zhang

Attribute-Based Encryption

Outsourcing the Re-encryption Key Generation: Flexible Ciphertext-
Policy Attribute-Based Proxy Re-encryption 301
Yutaka Kawai

Revocable Threshold Attribute-Based Signature against Signing Key Exposure	316
<i>Jianghong Wei, Xinyi Huang, Xuexian Hu, and Wenfen Liu</i>	
Fully Secure Online/Offline Predicate and Attribute-Based Encryption	331
<i>Pratish Datta, Ratna Dutta, and Sourav Mukhopadhyay</i>	

Mobile Security

A Rapid and Scalable Method for Android Application Repackaging Detection	349
<i>Sibei Jiao, Yao Cheng, Lingyun Ying, Purui Su, and Dengguo Feng</i>	
Comprehensive Analysis of the Android Google Play's Auto-update Policy	365
<i>Craig Sanders, Ayush Shah, and Shengzhi Zhang</i>	
IVDroid: Static Detection for Input Validation Vulnerability in Android Inter-component Communication	378
<i>Zhejun Fang, Qixu Liu, Yuqing Zhang, Kai Wang, and Zhiqiang Wang</i>	

Theory

New Constructions of T-function	395
<i>Dibyendu Roy, Ankita Chaturvedi, and Sourav Mukhopadhyay</i>	
A New Lattice-Based Threshold Attribute-Based Signature Scheme	406
<i>Qingbin Wang, Shaozhen Chen, and Aijun Ge</i>	
Hard Invalidation of Electronic Signatures	421
<i>Lucjan Hanzlik, Mirosław Kutylowski, and Moti Yung</i>	

Implementation

Lightweight Function Pointer Analysis	439
<i>Wei Zhang and Yu Zhang</i>	
Accelerating RSA with Fine-Grained Parallelism Using GPU	454
<i>Yang Yang, Zhi Guan, Huiping Sun, and Zhong Chen</i>	
On the Impacts of Mathematical Realization over Practical Security of Leakage Resilient Cryptographic Schemes	469
<i>Guangjun Fan, Yongbin Zhou, François-Xavier Standaert, and Dengguo Feng</i>	

Non-interactive Revocable Identity-Based Access Control over e-Healthcare Records	485
<i>Yunya Zhou, Jianwei Liu, Hua Deng, Bo Qin, and Lei Zhang</i>	
Efficient File Sharing in Electronic Health Records	499
<i>Clémentine Gritti, Willy Susilo, and Thomas Plantard</i>	
A Framework for Analyzing Verifiability in Traditional and Electronic Exams	514
<i>Jannik Dreier, Rosario Giustolisi, Ali Kassem, Pascal Lafourcade, and Gabriele Lenzini</i>	
 Privacy and Indistinguishability	
ADKAM: A-Diversity K-Anonymity Model via Microaggregation	533
<i>Liang Cheng, Shaoyin Cheng, and Fan Jiang</i>	
Visualizing Privacy Risks of Mobile Applications through a Privacy Meter	548
<i>Jina Kang, Hyounghick Kim, Yun Gyung Cheong, and Jun Ho Huh</i>	
One-Round Witness Indistinguishability from Indistinguishability Obfuscation	559
<i>Qihua Niu, Hongda Li, Guifang Huang, Bei Liang, and Fei Tang</i>	
 Author Index	 575

Information Security Practice and Experience
11th International Conference, ISPEC 2015, Beijing,
China, May 5-8, 2015, Proceedings
Lopez, J.; Wu, Y. (Eds.)
2015, XIV, 576 p. 76 illus., Softcover
ISBN: 978-3-319-17532-4