

Lucas C.K. Hui · S.H. Qing
Elaine Shi · S.M. Yiu (Eds.)

Information and Communications Security

16th International Conference, ICICS 2014
Hong Kong, China, December 16–17, 2014
Revised Selected Papers

Contents

Error-Tolerant Algebraic Side-Channel Attacks Using BEE	1
<i>Ling Song, Lei Hu, Siwei Sun, Zhang Zhang, Danping Shi, and Ronglin Hao</i>	
SEDB: Building Secure Database Services for Sensitive Data	16
<i>Quanwei Cai, Jingqiang Lin, Fengjun Li, and Qiong Xiao Wang</i>	
Mdaak: A Flexible and Efficient Framework for Direct Anonymous Attestation on Mobile Devices	31
<i>Qianying Zhang, Shijun Zhao, Li Xi, Wei Feng, and Dengguo Feng</i>	
Protecting Elliptic Curve Cryptography Against Memory Disclosure Attacks	49
<i>Yang Yang, Zhi Guan, Zhe Liu, and Zhong Chen</i>	
4P_VES: A Collusion-Resistant Accountable Virtual Economy System	61
<i>Hong Zhang, Xiaolei Dong, Zhenfu Cao, and Jiachen Shen</i>	
Privacy-Preserving Distance-Bounding Proof-of-Knowledge	74
<i>Ahmad Ahmadi and Reihaneh Safavi-Naini</i>	
Distance Lower Bounding	89
<i>Xifan Zheng, Reihaneh Safavi-Naini, and Hadi Ahmadi</i>	
Efficient Adaptive Oblivious Transfer Without q -type Assumptions in UC Framework	105
<i>Vandana Guleria and Ratna Dutta</i>	
TagDroid: Hybrid SSL Certificate Verification in Android	120
<i>Hui Liu, Yuanyuan Zhang, Hui Wang, Wenbo Yang, Juanru Li, and Dawu Gu</i>	
A Guess-Then-Algebraic Attack on LFSR-Based Stream Ciphers with Nonlinear Filter	132
<i>Xiao Zhong, Mingsheng Wang, Bin Zhang, and Shengbao Wu</i>	
A Private Lookup Protocol with Low Online Complexity for Secure Multiparty Computation	143
<i>Peeter Laud</i>	
Reverse Product-Scanning Multiplication and Squaring on 8-Bit AVR Processors	158
<i>Zhe Liu, Hwajeong Seo, Johann Großschädl, and Howon Kim</i>	

New Security Proof for the Boneh-Boyen IBE: Tight Reduction in Unbounded Multi-challenge Security	176
<i>Nuttapong Attrapadung, Goichiro Hanaoka, and Shota Yamada</i>	
Method for Determining Whether or not Text Information Is Leaked from Computer Display Through Electromagnetic Radiation.	191
<i>De-gang Sun, Jun Shi, Dong Wei, Meng Zhang, and Wei-qing Huang</i>	
How to Compare Selections of Points of Interest for Side-Channel Distinguishers in Practice?	200
<i>Yingxian Zheng, Yongbin Zhou, Zhenmei Yu, Chengyu Hu, and Hailong Zhang</i>	
Attribute Based Key-Insulated Signatures with Message Recovery.	215
<i>Y. Sreenivasa Rao and Ratna Dutta</i>	
XOR Based Non-monotone t -(k, n)*-Visual Cryptographic Schemes Using Linear Algebra	230
<i>Sabyasachi Dutta and Avishek Adhikari</i>	
A Visual One-Time Password Authentication Scheme Using Mobile Devices	243
<i>Yang-Wai Chow, Willy Susilo, Man Ho Au, and Ari Moesriami Barmawi</i>	
Secure and Efficient Scheme for Delegation of Signing Rights	258
<i>Rajeev Anand Sahu and Vishal Saraswat</i>	
Fully Secure Ciphertext-Policy Attribute Based Encryption with Security Mediator	274
<i>Yuechen Chen, Zoe L. Jiang, S.M. Yiu, Joseph K. Liu, Man Ho Au, and Xuan Wang</i>	
MOVTCHA: A CAPTCHA Based on Human Cognitive and Behavioral Features Analysis	290
<i>Asadullah Al Galib and Reihaneh Safavi-Naini</i>	
Security Analysis of EMV Channel Establishment Protocol in An Enhanced Security Model	305
<i>Yanfei Guo, Zhenfeng Zhang, Jiang Zhang, and Xuexian Hu</i>	
Author Index	321