

Contents

Security of Blind Discrete Log Signatures against Interactive Attacks	1
<i>Claus Peter Schnorr (Universität Frankfurt, Germany)</i>	
An Intelligent Intruder Model for Security Protocol Analysis	13
<i>Dongxi Liu, Xiaoyong Li, and Yingcai Bai (Shanghai Jiaotong University, China)</i>	
Primitive Polynomials over GF(2) – A Cryptologic Approach	23
<i>Kishan Chand Gupta and Subhamoy Maitra (Indian Statistical Institute, India)</i>	
Unconditionally-Secure Oblivious Transfer	35
<i>Bo Yang (Xidian University, China), Shixiong Zhu (Southwest Communications Institute of China), and Yumin Wang (Xidian University, China)</i>	
Cryptanalysis of the Improved User Efficient Blind Signatures	42
<i>Chin-Chen Chang and Iuon-Chang Lin (National Chung Cheng University, Taiwan)</i>	
Towards the Forgery of a Group Signature without Knowing the Group Center’s Secret	47
<i>Chin-Chen Chang and Kuo-Feng Hwang (National Chung Cheng University, Taiwan)</i>	
Evaluation of the Image Degradation for a Typical Watermarking Algorithm in the Block-DCT Domain	52
<i>Xiaochen Bo, Lincheng Shen, and Wensen Chang (National University of Defense Technology, China)</i>	
A Cyclic Window Algorithm for ECC Defined over Extension Fields	62
<i>Kazumaro Aoki (NTT Communications, Japan), Fumitaka Hoshino, and Tetsutaro Kobayashi (NTT Corporation, Japan)</i>	
Fast Scalar Multiplication on the Jacobian of a Family of Hyperelliptic Curves	74
<i>Fanguo Zhang, Futai Zhang, and Yumin Wang (Xidian University, China)</i>	
Attacks on Two Digital Signature Schemes Based on Error Correcting Codes	84
<i>Dingfeng Ye, Junhui Yang, Zongduo Dai, and Haiwen Ou (Chinese Academy of Sciences, China)</i>	

A Derivative of Digital Objects and Estimation of Default Risks in Electronic Commerce	90
<i>Kanta Matsuura (University of Tokyo, Japan)</i>	
A New Approach for Secure Multicast Routing in a Large Scale Network ...	95
<i>Young-Chul Shim (Hong-Ik University, Korea)</i>	
A Transaction Length-Sensitive Protocol Based on Altruistic Locking for Multilevel Secure Database Systems	107
<i>Hee-Wan Kim (Shamyook University, Korea),</i>	
<i>Hae-Kyung Rhee (Kyungin Women's College, Korea),</i>	
<i>Tai M. Chung, Young Ik Eom, and</i>	
<i>Ung-Mo Kim (Sungkyunkwan University, Korea)</i>	
Dealing with Uncertainties in Risk Analysis Using Belief Functions	119
<i>Sungbaek Cho and Zbigniew Ciechanowicz (University of London, UK)</i>	
RBAC for XML Document Stores	131
<i>Michael Hitchens and</i>	
<i>Vijay Varadharajan (Macquarie University, Australia)</i>	
Cheating Immune Secret Sharing	144
<i>Xian-Mo Zhang (University of Wollongong, Australia), and</i>	
<i>Josef Pieprzyk (Macquarie University, Australia)</i>	
Encryption Sticks (Randomats)	150
<i>Gideon Samid (Israel Institute of Technology, Israel)</i>	
Applying NCP Logic to the Analysis of SSL 3.0	155
<i>Zhimin Song and Sihan Qing (Chinese Academy of Sciences, China)</i>	
Performance of WTLS and Its Impact on an M-commerce Transaction	167
<i>Ian Herwono and</i>	
<i>Ingo Liebhardt (Aachen University of Technology, Germany)</i>	
Enforcing Obligation with Security Monitors	172
<i>Carlos Ribeiro, André Zúquete, and</i>	
<i>Paulo Ferreira (IST/INESC, Portugal)</i>	
Efficient Software Implementation for Finite Field Multiplication in Normal Basis	177
<i>Peng Ning (North Carolina State University, USA), and</i>	
<i>Yiqun Lisa Yin (NTT Multimedia Communications Labs, USA)</i>	
Playing Lottery on the Internet	189
<i>Jianying Zhou (Oracle Corporation, USA), and</i>	
<i>Chunfu Tan (Kent Ridge Digital Labs, Singapore)</i>	

Privacy Protection for Transactions of Digital Goods	202
<i>Feng Bao and Robert Deng (Kent Ridge Digital Labs, Singapore)</i>	
Equivalent Characterizations and Applications of Multi-output Correlation-Immune Boolean Functions	214
<i>Jie-lü Xu, Han-liang Xu, Yan Wang, and Shu-Wang Lü (Chinese Academy of Sciences, China)</i>	
Threshold Undeniable RSA Signature Scheme	221
<i>Guilin Wang, Sihan Qing, Mingsheng Wang (Chinese Academy of Sciences, China), and Zhanfei Zhou (Nihon University, Japan)</i>	
Two Simple Batch Verifying Multiple Digital Signatures	233
<i>Min-Shiang Hwang (Chaoyang University of Technology, Taiwan), Cheng-Chi Lee (National Chiao-Tung University, Taiwan), and Yuan-Liang Tang (Chaoyang University of Technology, Taiwan)</i>	
Square Attack on Reduced Camellia Cipher	238
<i>Yeping He and Sihan Qing (Chinese Academy of Sciences, China)</i>	
Generalization of Elliptic Curve Digital Signature Schemes	246
<i>Lin You (Hainan Normal University, Dalian University of Technology, China), Yi Xian Yang (Beijing University of Posts & Telecom, China), and Chun Qi Zhang (Beijing University of Posts & Telecom, China)</i>	
Reasoning about Accountability within Delegation	251
<i>Bruno Crispo (Cryptomathic S.p.A, Italy), and Giancarlo Ruffo (Università di Torino, Italy)</i>	
A Novel Data Hiding Method for Two-Color Images	261
<i>Gang Pan, Yijun Wu, and Zhaohui Wu (Zhejiang University, China)</i>	
An Identification Scheme Provably Secure against Reset Attack	271
<i>C.-H. Lee, X. Deng (City University of Hong Kong, China), and H. Zhu (Zhejiang University, China)</i>	
Estimating the Scalability of the Internet Key Exchange	280
<i>Sanna Kunnari (IP Security Competence Center, Finland)</i>	
An Efficient Information Flow Analysis of Recursive Programs Based on a Lattice Model of Security Classes	292
<i>Shigeta Kuninobu, Yoshiaki Takata, Hiroyuki Seki (Nara Institute of Science and Technology, Japan), and Katsuro Inoue (Osaka University, Japan)</i>	
Defeating Denial-of-Service Attacks on the Internet	304
<i>Baoqing Ye (Verizon Labs, USA)</i>	

A Role-Based Access Control Model and Implementation for Data-Centric Enterprise Applications	316
<i>Dianlong Zhang, Harald Lukhaub, and Werner Zorn (University of Karlsruhe, Germany)</i>	
A Unified Methodology for Verification and Synthesis of Firewall Configurations	328
<i>Yongyuth Permpoontanalarp and Chaiwat Rujimethabhas (King Mongkut's University of Technology, Thailand)</i>	
Quantifying Network Denial of Service: A Location Service Case Study ...	340
<i>Yan Chen, Adam Bargteil, David Bindel, Randy H. Katz, and John Kubiataowicz (University of California, Berkeley, USA)</i>	
A Public Key Cryptosystem Based on the Subgroup Membership Problem	352
<i>Juan Manuel González Nieto, Colin Boyd, and Ed Dawson (Queensland University of Technology, Australia)</i>	
On a Network Security Model for the Secure Information Flow on Multilevel Secure Network	364
<i>Ki-Yoong Hong (KSIGN and SECUBE, Korea), and Chul Kim (Kwangwoon University, Korea)</i>	
NIDS Research Based on Artificial Immunology	371
<i>Wenjian Luo, Xianbin Cao, and Xufa Wang (University of Science and Technology of China)</i>	
AMBAR Protocol: Access Management Based on Authorization Reduction	376
<i>Oscar Cánovas and Antonio F. Gómez (University of Murcia, Spain)</i>	
Chinese Remainder Theorem Based Hierarchical Access Control for Secure Group Communication	381
<i>Xukai Zou, Byrav Ramamurthy (University of Nebraska-Lincoln, USA), and Spyros S. Magliveras (Florida Atlantic University, USA)</i>	
Dispatching Mobile Agents with Secure Routes in Parallel	386
<i>Yan Wang and Kian-Lee Tan (National University of Singapore)</i>	
TH-SMS: Security Management System in Advanced Computational Infrastructure	398
<i>Yu Chen, Qian Fang, Zhihui Du, Zhenchun Huang, and Sanli Li (Tsinghua University, China)</i>	

Cryptography and Middleware Security	408
<i>Ulrich Lang (University of Cambridge, UK),</i>	
<i>Dieter Gollmann (Microsoft Research, Cambridge, UK), and</i>	
<i>Rudolf Schreiner (ObjectSecurity Ltd., UK)</i>	
Cryptanalysis of the Hwang-Rao Secret Error-Correcting Code Schemes ...	419
<i>Kencheng Zeng (Chinese Academy of Sciences, China),</i>	
<i>Chung-Huang Yang (National Kaohsiung University of</i>	
<i>Science and Technology, Taiwan),</i>	
<i>and T.R.N. Rao (University of Louisiana, USA)</i>	
A Role-Based Model for Access Control in Database Federations	429
<i>Eric Disson, Danielle Boulanger, and</i>	
<i>Gilles Dubois (Université Jean Moulin Lyon 3, France)</i>	
A Useful Intrusion Detection System Prototype to Monitor	
Multi-processes Based on System Calls	441
<i>Hongpei Li, Lianli Chang, and</i>	
<i>Xinmei Wang (Xidian University, China)</i>	
A Digital Nominative Proxy Signature Scheme for Mobile	
Communication	451
<i>Hee-Un Park and Im-Yeong Lee (Soonchunhyang University, Korea)</i>	
Hierarchical Simulation Model with Animation for Large	
Network Security	456
<i>Mi Ra Yi and Tae Ho Cho (Sungkyunkwan University, Korea)</i>	
Fair Electronic Cash Based on a Group Signature Scheme	461
<i>Greg Maitland and</i>	
<i>Colin Boyd (Queensland University of Technology, Australia)</i>	
Fair Exchange of Digital Signatures with Offline Trusted Third Party	466
<i>Chuan-Kun Wu (Australian National University), and</i>	
<i>Vijay Varadharajan (Macquarie University, Australia)</i>	
SECUSIM: A Tool for the Cyber-Attack Simulation	471
<i>Jong Sou Park, Jang-Se Lee, Hwan Kuk Kim, Jeong-Rye Jeong,</i>	
<i>Dong-Bok Yeom, and Sung-Do Chi (Hangkong University, Korea)</i>	
A New Semantics of Authentication Logic	476
<i>Yifa Li (University of Information Engineering, China)</i>	
Robust and Fragile Watermarking Techniques for Documents Using	
Bi-directional Diagonal Profiles	483
<i>Ji Hwan Park, Sook Ee Jeong, and</i>	
<i>Chang Soo Kim (Pukyong National University, Korea)</i>	

Redundancy, Obscurity, Self-Containment & Independence495
 Seenil Gram (USA)

Author Index 503



<http://www.springer.com/978-3-540-42880-0>

Information and Communications Security
Third International Conference, ICICS 2001, Xian, China,
November 13-16, 2001. Proceedings
Okamoto, T.; Zhou, J. (Eds.)
2001, XIV, 510 p., Softcover
ISBN: 978-3-540-42880-0