Contents

Security of Blind Discrete Log Signatures against Interactive Attacks 1
Claus Peter Schnorr (Universität Frankfurt, Germany)

An Intelligent Intruder Model for Security Protocol Analysis 13
Dongxi Liu, Xiaoyong Li, and
Yingcai Bai (Shanghai Jiaotong University, China)

Primitive Polynomials over GF(2) – A Cryptologic Approach 23
Kishan Chand Gupta and
Subhamoy Maitra (Indian Statistical Institute, India)

Unconditionally-Secure Oblivious Transfer 35
Bo Yang (Xidian University, China),
Shixiong Zhu (Southwest Communications Institute of China), and
Yumin Wang (Xidian University, China)

Cryptanalysis of the Improved User Efficient Blind Signatures 42
Chin-Chen Chang and
Iuon-Chang Lin (National Chung Cheng University, Taiwan)

Towards the Forgery of a Group Signature without Knowing
the Group Center's Secret 47
Chin-Chen Chang and
Kuo-Feng Hwang (National Chung Cheng University, Taiwan)

Evaluation of the Image Degradation for a Typical Watermarking
Algorithm in the Block-DCT Domain 52
Xiaochen Bo, Lincheng Shen, and
Wensen Chang (National University of Defense Technology, China)

A Cyclic Window Algorithm for ECC Defined over Extension Fields 62
Kazumaro Aoki (NTT Communications, Japan),
Fumitaka Hoshino, and Tetsutaro Kobayashi (NTT Corporation, Japan)

Fast Scalar Multiplication on the Jacobian of a Family
of Hyperelliptic Curves 74
Fangguo Zhang, Futai Zhang, and
Yumin Wang (Xidian University, China)

Attacks on Two Digital Signature Schemes Based on Error
Correcting Codes 84
Dingfeng Ye, Junhui Yang, Zongduo Dai, and
Haiwen Ou (Chinese Academy of Sciences, China)

A Derivative of Digital Objects and Estimation of Default Risks in Electronic Commerce 90
Kanta Matsuura (University of Tokyo, Japan)

A New Approach for Secure Multicast Routing in a Large Scale Network ... 95
Young-Chul Shim (Hong-Ik University, Korea)

A Transaction Length-Sensitive Protocol Based on Altruistic Locking for Multilevel Secure Database Systems 107
Hee-Wan Kim (Shamyook University, Korea),
Hae-Kyung Rhee (Kyungin Women's College, Korea),
Tai M. Chung, Young Ik Eom, and
Ung-Mo Kim (Sungkyunkwan University, Korea)

Dealing with Uncertainties in Risk Analysis Using Belief Functions 119
Sungbaek Cho and Zbigniew Ciechanowicz (University of London, UK)

RBAC for XML Document Stores 131
Michael Hitchens and
Vijay Varadharajan (Macquarie University, Australia)

Cheating Immune Secret Sharing 144
Xian-Mo Zhang (University of Wollongong, Australia), and
Josef Pieprzyk (Macquarie University, Australia)

Encryption Sticks (Randomats) 150
Gideon Samid (Israel Institute of Technology, Israel)

Applying NCP Logic to the Analysis of SSL 3.0 155
Zhimin Song and Sihan Qing (Chinese Academy of Sciences, China)

Performance of WTLS and Its Impact on an M-commerce Transaction 167
Ian Herwono and
Ingo Liebhardt (Aachen University of Technology, Germany)

Enforcing Obligation with Security Monitors 172
Carlos Ribeiro, André Zúquete, and
Paulo Ferreira (IST/INESC, Portugal)

Efficient Software Implementation for Finite Field Multiplication in Normal Basis 177
Peng Ning (North Carolina State University, USA), and
Yiqun Lisa Yin (NTT Multimedia Communications Labs, USA)

Playing Lottery on the Internet 189
Jianying Zhou (Oracle Corporation, USA), and
Chunfu Tan (Kent Ridge Digital Labs, Singapore)

Privacy Protection for Transactions of Digital Goods 202
Feng Bao and Robert Deng (Kent Ridge Digital Labs, Singapore)

Equivalent Characterizations and Applications of Multi-output Correlation-Immune Boolean Functions 214
Jie-lü Xu, Han-liang Xu, Yan Wang, and Shu-Wang Lü (Chinese Academy of Sciences, China)

Threshold Undeniable RSA Signature Scheme 221
Guilin Wang, Sihan Qing, Mingsheng Wang (Chinese Academy of Sciences, China), and Zhanfei Zhou (Nihon University, Japan)

Two Simple Batch Verifying Multiple Digital Signatures 233
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)

Square Attack on Reduced Camellia Cipher 238
Yeping He and Sihan Qing (Chinese Academy of Sciences, China)

Generalization of Elliptic Curve Digital Signature Schemes 246
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)

Reasoning about Accountability within Delegation 251
Bruno Crispo (Cryptomathic S.p.A, Italy), and Giancarlo Ruffo (Università di Torino, Italy)

A Novel Data Hiding Method for Two-Color Images 261
Gang Pan, Yijun Wu, and Zhaohui Wu (Zhejiang University, China)

An Identification Scheme Provably Secure against Reset Attack 271
C.-H. Lee, X. Deng (City University of Hong Kong, China), and H. Zhu (Zhejiang University, China)

Estimating the Scalability of the Internet Key Exchange 280
Sanna Kunnari (IP Security Competence Center, Finland)

An Efficient Information Flow Analysis of Recursive Programs Based on a Lattice Model of Security Classes 292
Shigeta Kuninobu, Yoshiaki Takata, Hiroyuki Seki (Nara Institute of Science and Technology, Japan), and Katsuro Inoue (Osaka University, Japan)

Defeating Denial-of-Service Attacks on the Internet 304
Baoqing Ye (Verizon Labs, USA)

A Role-Based Access Control Model and Implementation for Data-Centric Enterprise Applications 316
Dianlong Zhang, Harald Lukhaub, and Werner Zorn (University of Karlsruhe, Germany)

A Unified Methodology for Verification and Synthesis of Firewall Configurations 328
Yongyuth Permpoontanalarp and Chaiwat Rujimethabhas (King Mongkut's University of Technology, Thailand)

Quantifying Network Denial of Service: A Location Service Case Study ... 340
Yan Chen, Adam Bargteil, David Bindel, Randy H. Katz, and John Kubiatowicz (University of California, Berkeley, USA)

A Public Key Cryptosystem Based on the Subgroup Membership Problem 352
Juan Manuel González Nieto, Colin Boyd, and Ed Dawson (Queensland University of Technology, Australia)

On a Network Security Model for the Secure Information Flow on Multilevel Secure Network 364
Ki-Yoong Hong (KSIGN and SECUVE, Korea), and Chul Kim (Kwangwoon University, Korea)

NIDS Research Based on Artificial Immunology 371
Wenjian Luo, Xianbin Cao, and Xufa Wang (University of Science and Technology of China)

AMBAR Protocol: Access Management Based on Authorization Reduction 376
Oscar Cánovas and Antonio F. Gómez (University of Murcia, Spain)

Chinese Remainder Theorem Based Hierarchical Access Control for Secure Group Communication 381
Xukai Zou, Byrav Ramamurthy (University of Nebraska-Lincoln, USA), and Spyros S. Magliveras (Florida Atlantic University, USA)

Dispatching Mobile Agents with Secure Routes in Parallel 386
Yan Wang and Kian-Lee Tan (National University of Singapore)

TH-SMS: Security Management System in Advanced Computational Infrastructure 398
Yu Chen, Qian Fang, Zhihui Du, Zhenchun Huang, and Sanli Li (Tsinghua University, China)

Cryptography and Middleware Security 408
Ulrich Lang (University of Cambridge, UK),
Dieter Gollmann (Microsoft Research, Cambridge, UK), and
Rudolf Schreiner (ObjectSecurity Ltd., UK)

Cryptanalysis of the Hwang-Rao Secret Error-Correcting Code Schemes ... 419
Kencheng Zeng (Chinese Academy of Sciences, China),
Chung-Huang Yang (National Kaohsiung University of
Science and Technology, Taiwan),
and T.R.N. Rao (University of Louisiana, USA)

A Role-Based Model for Access Control in Database Federations 429
Eric Disson, Danielle Boulanger, and
Gilles Dubois (Université Jean Moulin Lyon 3, France)

A Useful Intrusion Detection System Prototype to Monitor
Multi-processes Based on System Calls 441
Hongpei Li, Lianli Chang, and
Xinmei Wang (Xidian University, China)

A Digital Nominative Proxy Signature Scheme for Mobile
Communication 451
Hee-Un Park and Im-Yeong Lee (Soonchunhyang University, Korea)

Hierarchical Simulation Model with Animation for Large
Network Security 456
Mi Ra Yi and Tae Ho Cho (Sungkyunkwan University, Korea)

Fair Electronic Cash Based on a Group Signature Scheme 461
Greg Maitland and
Colin Boyd (Queensland University of Technology, Australia)

Fair Exchange of Digital Signatures with Offline Trusted Third Party 466
Chuan-Kun Wu (Australian National University), and
Vijay Varadharajan (Macquarie University, Australia)

SECUSIM: A Tool for the Cyber-Attack Simulation 471
Jong Sou Park, Jang-Se Lee, Hwan Kuk Kim, Jeong-Rye Jeong,
Dong-Bok Yeom, and Sung-Do Chi (Hangkong University, Korea)

A New Semantics of Authentication Logic 476
Yifa Li (University of Information Engineering, China)

Robust and Fragile Watermarking Techniques for Documents Using
Bi-directional Diagonal Profiles 483
Ji Hwan Park, Sook Ee Jeong, and
Chang Soo Kim (Pukyong National University, Korea)

Redundancy, Obscurity, Self-Containment & Independence 495
Seenil Gram (USA)

Author Index 503