

Table of Contents

System Security I

Defenses against the Truncation of Computation Results of Free-Roaming Agents	1
<i>Jeff S.L. Cheng and Victor K. Wei</i>	
A Distributed Dynamic μ Firewall Architecture with Mobile Agents and KeyNote Trust Management System	13
<i>Hai Jin, Feng Xian, Zongfen Han, and Shengli Li</i>	
Encoding Function Pointers and Memory Arrangement Checking against Buffer Overflow Attack	25
<i>Changwoo Pyo and Gyungho Lee</i>	
An Evaluation of Different IP Traceback Approaches	37
<i>Vadim Kuznetsov, Helena Sandström, and Andrei Simkin</i>	
Security against Inference Attacks on Negative Information in Object-Oriented Databases	49
<i>Yasunori Ishihara, Shuichiro Ako, and Toru Fujiwara</i>	

Cryptosystem I

Robust Key-Evolving Public Key Encryption Schemes	61
<i>Wen-Guey Tzeng and Zhi-Jia Tzeng</i>	
A Group Signature Scheme Committing the Group	73
<i>Toru Nakanishi, Masayuki Tao, and Yuji Sugiyama</i>	
Unconditionally Secure Key Insulated Cryptosystems: Models, Bounds and Constructions	85
<i>Yumiko Hanaoka, Goichiro Hanaoka, Junji Shikata, and Hideki Imai</i>	
Anonymous Fingerprinting as Secure as the Bilinear Diffie-Hellman Assumption	97
<i>Myungsun Kim, Jongseong Kim, and Kwangjo Kim</i>	
Reducing the Memory Complexity of Type-Inference Algorithms	109
<i>David Naccache, Alexei Tchoulkine, Christophe Tymen, and Elena Trichina</i>	

Security Protocol I

The Risks of Compromising Secret Information	122
<i>Kyungah Shim</i>	

Password-Authenticated Key Exchange between Clients with Different Passwords	134
<i>Jin Wook Byun, Ik Rae Jeong, Dong Hoon Lee, and Chang-Seop Park</i>	

Robust, Privacy Protecting and Publicly Verifiable Sealed-Bid Auction . . .	147
<i>Kun Peng, Colin Boyd, Ed Dawson, and Kapali Viswanathan</i>	

Attacking Predictable IPsec ESP Initialization Vectors	160
<i>Sami Vaarala, Antti Nuopponen, and Teemupekka Virtanen</i>	

Fingerprinting & Watermarking

An ID Coding Scheme for Fingerprinting, Randomized c -Secure CRT Code	173
<i>Hajime Watanabe and Takashi Kitagawa</i>	

A Robust Block Oriented Watermarking Scheme in Spatial Domain	184
<i>Tanmoy Kanti Das and Subhamoy Maitra</i>	

A Flexibly Revocable Key-Distribution Scheme for Efficient Black-Box Tracing	197
<i>Tatsuyuki Matsushita</i>	

Efficient Implementation of Algorithms

Low Complexity Bit Serial Systolic Multipliers over $GF(2^m)$ for Three Classes of Finite Fields	209
<i>Soonhak Kwon</i>	

Fast Elliptic Curve Multiplications with SIMD Operations	217
<i>Tetsuya Izu and Tsuyoshi Takagi</i>	

Further Results on Multiples of Primitive Polynomials and Their Products over $GF(2)$	231
<i>Ayineedi Venkateswarlu and Subhamoy Maitra</i>	

System Security II

A Secure Object Sharing Scheme for Java Card	243
<i>Junqi Zhang, Vijay Varadharajan, and Yi Mu</i>	

IDS Interoperability and Correlation Using IDMEF and Commodity Systems	252
<i>Nathan Carey, Andrew Clark, and George Mohay</i>	

A Synthetic Fraud Data Generation Methodology	265
<i>Emilie Lundin, Håkan Kvarnström, and Erland Jonsson</i>	
User Interaction Design for Secure Systems	278
<i>Ka-Ping Yee</i>	
Using Independent Auditors as Intrusion Detection Systems	291
<i>Jesus Molina and William Arbaugh</i>	

Cryptosystem II

Cellular Automata Based Cryptosystem (<i>CAC</i>)	303
<i>Subhayan Sen, Chandrama Shaw, Dipanwita Roy Chowdhuri, Niloy Ganguly, and P. Pal Chaudhuri</i>	
New Weak-Key Classes of IDEA	315
<i>Alex Biryukov, Jorge Nakahara Jr, Bart Preneel, and Joos Vandewalle</i>	
Risks with Raw-Key Masking – The Security Evaluation of <i>2-Key XCBC</i>	327
<i>Soichi Furuya and Kouichi Sakurai</i>	
A New Statistical Testing for Symmetric Ciphers and Hash Functions	342
<i>Eric Filiol</i>	
Message Authentication Codes with Error Correcting Capabilities	354
<i>Charles C.Y. Lam, Guang Gong, and Scott A. Vanstone</i>	

Access Control

The Consistency of an Access Control List	367
<i>Shou-peng Li, Shi-zhong Wu, and Tao Guo</i>	
Knowledge-Based Modeling and Simulation of Network Access Control Mechanisms Representing Security Policies	374
<i>Jong-Young Koh, Mi-Ra Yi, Tae-Ho Cho, Hyung-Jong Kim, and Hong-Geun Kim</i>	
A Specification Language for Distributed Policy Control	386
<i>Shigeta Kuninobu, Yoshiaki Takata, Daigo Taguchi, Masayuki Nakae, and Hiroyuki Seki</i>	
Access Control Infrastructure for Digital Objects	399
<i>Javier López, Antonio Maña, Ernesto Pimentel, José M. Troya, and Mariemma I. Yagüe</i>	

Security Protocol II

Distributed Key Generation as a Component of an Integrated Protocol ...	411
<i>Cheng-Kang Chu and Wen-Guey Tzeng</i>	

A Secure Agent-Mediated Payment Protocol	422
<i>Xiaolin Pang, Kian-Lee Tan, Yan Wang, and Jian Ren</i>	
Cryptanalysis & Cryptographic Techniques	
Tensor Transform of Boolean Functions and Related Algebraic and Probabilistic Properties	434
<i>Alexander Kholosha and Henk C.A. van Tilborg</i>	
Related-Cipher Attacks	447
<i>Hongjun Wu</i>	
A Chosen Plaintext Linear Attack on Block Cipher CIKS-1	456
<i>Changhoon Lee, Deukjo Hong, Sungjae Lee, Sangjin Lee, Hyungjin Yang, and Jongin Lim</i>	
Ideal Threshold Schemes from Orthogonal Arrays	469
<i>Josef Pieprzyk and Xiam-Mo Zhang</i>	
Cryptanalysis of the Reduced-Round RC6	480
<i>Atsuko Miyaji and Masao Nonaka</i>	
Author Index	495