

# Table of Contents

## Intrusion Detection and Tamper Resistance

Real-Time Intruder Tracing through Self-Replication .....	1
<i>Heejin Jang, Sangwook Kim</i>	
On the Difficulty of Protecting Private Keys in Software .....	17
<i>Taekyoung Kwon</i>	
Intrusion Detection with Support Vector Machines and Generative Models .....	32
<i>John S. Baras, Maben Rabi</i>	

## Cryptographic Algorithm and Attack Implementation

Small and High-Speed Hardware Architectures for the 3GPP Standard Cipher KASUMI .....	48
<i>Akashi Satoh, Sumio Morioka</i>	
Fast Software Implementations of SC2000 .....	63
<i>Helger Lipmaa</i>	
Comparative Analysis of the Hardware Implementations of Hash Functions SHA-1 and SHA-512 .....	75
<i>Tim Grembowski, Roar Lien, Kris Gaj, Nghi Nguyen, Peter Bellows, Jaroslav Flidr, Tom Lehman, Brian Schott</i>	
Implementation of Chosen-Ciphertext Attacks against PGP and GnuPG ..	90
<i>Kahil Jallad, Jonathan Katz, Bruce Schneier</i>	

## Access Control and Trust Management (I)

Role-Based Access Control for E-commerce Sea-of-Data Applications .....	102
<i>G. Navarro, S. Robles, J. Borrell</i>	
An Access Control Model for Tree Data Structures .....	117
<i>Alban Gabillon, Manuel Munier, Jean-Jacques Bascou, Laurent Gallon, Emmanuel Bruno</i>	
A New Design of Privilege Management Infrastructure for Organizations Using Outsourced PKI .....	136
<i>Ed Dawson, Javier Lopez, Jose A. Montenegro, Eiji Okamoto</i>	

## Authentication and Privacy

Password Authenticated Key Exchange Based on RSA for Imbalanced Wireless Networks . . . . .	150
<i>Feng Zhu, Duncan S. Wong, Agnes H. Chan, Robbie Ye</i>	
Quantifying Privacy Leakage through Answering Database Queries . . . . .	162
<i>Tsan-sheng Hsu, Churn-Jung Liau, Da-Wei Wang, Jeremy K.-P. Chen</i>	
A New Offline Privacy Protecting E-cash System with Revokable Anonymity . . . . .	177
<i>Weidong Qiu, Kefei Chen, Dawu Gu</i>	

## E-commerce Protocols (I)

Receipt-Free Sealed-Bid Auction . . . . .	191
<i>Masayuki Abe, Koutarou Suzuki</i>	
Exclusion-Freeness in Multi-party Exchange Protocols . . . . .	200
<i>Nicolás González-Deleito, Olivier Markowitch</i>	
A Realistic Protocol for Multi-party Certified Electronic Mail . . . . .	210
<i>Josep Lluís Ferrer-Gomila, Magdalena Payeras-Capellà, Llorenç Huguet-Rotger</i>	

## Signature Schemes

A Nyberg-Rueppel Signature for Multiple Messages and Its Batch Verification . . . . .	220
<i>Shunsuke Araki</i>	
Comments to the UNCITRAL Model Law on Electronic Signatures . . . . .	229
<i>Apol·lònia Martínez-Nadal, Josep Lluís Ferrer-Gomila</i>	
An Anonymous Loan System Based on Group Signature Scheme . . . . .	244
<i>Rie Shigetomi, Akira Otsuka, Takahide Ogawa, Hideki Imai</i>	
Traceability Schemes for Signed Documents . . . . .	257
<i>Shoko Yonezawa, Goichiro Hanaoka, Junji Shikata, Hideki Imai</i>	

## Cryptography (I)

Proofs of Knowledge for Non-monotone Discrete-Log Formulae and Applications . . . . .	272
<i>Emmanuel Bresson, Jacques Stern</i>	
Inversion/Division Systolic Architecture for Public-Key Cryptosystems in $GF(2^m)$ . . . . .	289
<i>Nam-Yeun Kim, Dae-Ghon Kho, Kee-Young Yoo</i>	

Efficient Bit Serial Multiplication Using Optimal Normal Bases of Type II in $GF(2^m)$ .....	300
<i>Soonhak Kwon, Heuisu Ryu</i>	

## Access Control and Trust Management (II)

Conditional Cryptographic Delegation for P2P Data Sharing .....	309
<i>Yuji Watanabe, Masayuki Numao</i>	
Certification of Public Keys within an Identity Based System .....	322
<i>L. Chen, K. Harrison, A. Moss, D. Soldera, N.P. Smart</i>	
A New Public Key Cryptosystem for Constrained Hardware .....	334
<i>Jiande Zheng</i>	

## Key Management

A Distributed and Computationally Secure Key Distribution Scheme .....	342
<i>Vanesa Daza, Javier Herranz, Carles Padró, Germán Sáez</i>	
On Optimal Hash Tree Traversal for Interval Time-Stamping .....	357
<i>Helger Lipmaa</i>	
An Efficient Dynamic and Distributed Cryptographic Accumulator .....	372
<i>Michael T. Goodrich, Roberto Tamassia, Jasminka Hasić</i>	

## Security Analysis

A Second-Order DPA Attack Breaks a Window-Method Based Countermeasure against Side Channel Attacks .....	389
<i>Katsuyuki Okeya, Kouichi Sakurai</i>	
Parallelizable Elliptic Curve Point Multiplication Method with Resistance against Side-Channel Attacks .....	402
<i>Bodo Möller</i>	
Automated Analysis of Some Security Mechanisms of SCEP .....	414
<i>Fabio Martinelli, Marinella Petrocchi, Anna Vaccarelli</i>	
An Attack on a Protocol for Certified Delivery .....	428
<i>José R.M. Monteiro, Ricardo Dahab</i>	

## E-commerce Protocols (II)

Oblivious Counter and Majority Protocol .....	437
<i>Hiroaki Kikuchi</i>	

Efficient Mental Card Shuffling via Optimised Arbitrary-Sized  
Benes Permutation Network . . . . . 446  
*Wai Han Soo, Azman Samsudin, Alwyn Goh*

Fingerprinting Concatenated Codes with Efficient Identification . . . . . 459  
*M. Fernandez, M. Soriano*

**Cryptography (II)**

A Provably Secure Additive and Multiplicative Privacy  
Homomorphism . . . . . 471  
*Josep Domingo-Ferrer*

Algorithms for Efficient Simultaneous Elliptic Scalar  
Multiplication with Reduced Joint Hamming Weight  
Representation of Scalars . . . . . 484  
*Yasuyuki Sakai, Kouichi Sakurai*

**Author Index** . . . . . 501