

Table of Contents

Network Security I

Protecting Confidentiality against Trojan Horse Programs in Discretionary Access Control System	1
<i>Adrian Spalka, Armin B. Cremers, and Hartmut Lehmler</i>	
Towards a New Authorisation Paradigm for Extranets	18
<i>Richard Au, Mark Looi, and Paul Ashley</i>	
Custom Safety Policies in Safe Erlang	30
<i>Lawrie Brown</i>	

Public Key Cryptography

A Proposal of a New Public Key Cryptosystem Using Matrices over a Ring	41
<i>Heajoung Yoo, Seokhie Hong, Sangjin Lee, Jongin Lim, Okyeon Yi, and Maenghee Sung</i>	
Secure Length-Saving ElGamal Encryption under the Computational Diffie-Hellman Assumption	49
<i>Joonsang Baek, Byoungcheon Lee, and Kwangjo Kim</i>	
Efficient Scalar Multiplications on Elliptic Curves without Repeated Doublings and Their Practical Performance	59
<i>Yasuyuki Sakai and Kouichi Sakurai</i>	

Network Security II

High Performance Agile Crypto Modules	74
<i>Chandana G. Gamage, Jussipekka Leiwo, and Yuliang Zheng</i>	
A Three-Party HTTP Proxy to Support Internet Content Regulation	89
<i>Agung Prasetijo, Paul Ashley, Mark Looi, Andrew Clark, and Gary Gaskell</i>	

Cryptographic Implementation Issues

Cryptanalysis of the m -Permutation Protection Schemes	97
<i>Hongjun Wu, Feng Bao, Dingfeng Ye, and Robert H. Deng</i>	
An Implementation of Bitsliced DES on the Pentium MMX TM Processor	112
<i>Lauren May, Lyta Penna, and Andrew Clark</i>	

Electronic Commerce I

Securing Large E-Commerce Networks	123
<i>Panagiotis Sklavos, Aggelos Varvitsiotis, and Despina Polemi</i>	
Passive Entities: A Strategy for Electronic Payment Design	134
<i>Ernest Foo and Colin Boyd</i>	

Key Recovery

Key Recovery System for the Commercial Environment	149
<i>Juanma González Nieto, Kapali Viswanathan, Colin Boyd, and Ed Dawson</i>	
A Key Escrow Scheme with Time-Limited Monitoring for One-Way Communication	163
<i>Masayuki Abe and Masayuki Kanda</i>	

Public Key Infrastructure

Key Management for Secure Multicast with Dynamic Controller	178
<i>Hartono Kurnio, Rei Safavi-Naini, Willy Susilo, and Huaxiong Wang</i>	
PKI Seeks a Trusting Relationship	191
<i>Audun Jøsang, Ingar Glenn Pedersen, and Dean Povey</i>	
The PKI Specification Dilemma: A Formal Solution	206
<i>Maris A. Ozols, Marie Henderson, Chuchang Liu, and Tony Cant</i>	

Boolean Functions

Iterative Probabilistic Cryptanalysis of RC4 Keystream Generator	220
<i>Jovan Dj. Golić</i>	
Security Weaknesses in a Randomized Stream Cipher	234
<i>Niels Ferguson, Bruce Schneier, and David Wagner</i>	
Two-Stage Optimisation in the Design of Boolean Functions	242
<i>John A. Clark and Jeremy L. Jacob</i>	

Intrusion Detection

A Novel Engine for Various Intrusion Detection Methods	255
<i>Z. Hui and T.H. Daniel Tan</i>	

Codes

Construction and Categories of Codes	266
<i>G.R. Blakley, I. Borosh, and A. Klappenecker</i>	

Digital Signatures I

- Cryptanalysis of Polynomial Authentication and Signature Scheme 278
Hongjun Wu, Feng Bao, Dingfeng Ye, and Robert H. Deng
- Secure Transactions with Mobile Agents in Hostile Environments 289
*Panayiotis Kotzanikolaou, Mike Burmester,
 and Vassilios Chrissikopoulos*
- A Multisignature Scheme with Message Flexibility, Order Flexibility and
 Order Verifiability 298
Shirow Mitomi and Atsuko Miyaji

Secret Sharing I

- Light Weight Broadcast Exclusion Using Secret Sharing 313
Natsume Matsuzaki, Jun Anzai, and Tsutomu Matsumoto
- Cheating Prevention in Secret Sharing 328
Hossein Ghodosi and Josef Pieprzyk
- On Multiplicative Secret Sharing Schemes 342
Huaxiong Wang, Kwok Yan Lam, Guo-Zhen Xiao, and Huanhui Zhao

Digital Signatures II

- On the Security of the RSA-Based Multisignature Scheme for Various
 Group Structures 352
Hiroshi Doi, Masahiro Mambo, and Eiji Okamoto
- Fail-Stop Confirmer Signatures 368
Yi Mu and Vijay Varadharajan
- An Extremely Small and Efficient Identification Scheme 378
William D. Banks, Daniel Lieman, and Igor E. Shparlinski

Protocols

- An Anonymous Electronic Bidding Protocol Based on a New Convertible
 Group Signature Scheme 385
Kouichi Sakurai and Shingo Miyazaki
- AKA Protocols for Mobile Communications 400
KookHwi Lee and SangJae Moon

Electronic Commerce II

- A Three Phased Schema for Sealed Bid Auction System Design 412
Kapali Viswanathan, Colin Boyd, and Ed Dawson

An Online Public Auction Protocol Protecting Bidder Privacy 427
Khanh Quoc Nguyen and Jacques Traoré

Secret Sharing II

Algorithms to Speed Up Computations in Threshold RSA 443
Brian King

Sharing Block Ciphers 457
Ernie Brickell, Giovanni Di Crescenzo, and Yair Frankel

Keynote Papers

All Sail, No Anchor, I: Cryptography, Risk, and e-Commerce 471
Bob Blakley and G.R. Blakley

Professional Ethics in a Security and Privacy Context - the Perspective of
a National Computing Society 477
Alan Underwood

Author Index 487