

Table of Contents

Network/Computer Security

Impacts of Security Protocols on Real-Time Multimedia Communications.....	1
<i>Kihun Hong, Souhwan Jung, Luigi Lo Iacono, and Christoph Ruland</i>	
An Improvement on Privacy and Authentication in GSM.....	14
<i>Young Jae Choi and Soon Ja Kim</i>	
Encrypted Watermarks and Linux Laptop Security	27
<i>Markku-Juhani O. Saarinen</i>	
Inconsistency Detection of Authorization Policies in Distributed Component Environment	39
<i>Chang-Joo Moon and Hoh Peter In</i>	

Public Key Schemes I

Custodian-Hiding Verifiable Encryption.....	51
<i>Joseph K. Liu, Victor K. Wei, and Duncan S. Wong</i>	
Proving Key Usage.....	65
<i>Malek Bechlaghem and Vincent Rijmen</i>	
Public Key Encryption with Conjunctive Field Keyword Search.....	73
<i>Dong Jin Park, Kihyun Kim, and Pil Joong Lee</i>	

Intrusion Detection I

A Probabilistic Method for Detecting Anomalous Program Behavior.....	87
<i>Kohei Tatara, Toshihiro Tabata, and Kouichi Sakurai</i>	
Service Discrimination and Audit File Reduction for Effective Intrusion Detection	99
<i>Fernando Godínez, Dieter Hutter, and Raúl Monroy</i>	
IDS False Alarm Filtering Using KNN Classifier	114
<i>Kwok Ho Law and Lam For Kwok</i>	

Watermarking/Anti-spamming

Content-Based Synchronization Using the Local Invariant Feature for Robust Watermarking	122
<i>Hae-Yeoun Lee, Jong-Tae Kim, Heung-Kyu Lee, and Young-Ho Suh</i>	

Some Fitting of Naive Bayesian Spam Filtering for Japanese Environment	135
<i>Manabu Iwanaga, Toshihiro Tabata, and Kouichi Sakurai</i>	

Public Key Schemes II

Efficient Authenticated Key Agreement Protocol for Dynamic Groups	144
<i>Kui Ren, Hyunrok Lee, Kwangjo Kim, and Taewhan Yoo</i>	
A Ring Signature Scheme Using Bilinear Pairings	160
<i>Jing Xu, Zhenfeng Zhang, and Dengguo Feng</i>	
Verifiable Pairing and Its Applications	170
<i>Sherman S.M. Chow</i>	

Intrusion Detection II

Improving the Performance of Signature-Based Network Intrusion Detection Sensors by Multi-threading	188
<i>Bart Haagdorens, Tim Vermeiren, and Marnix Goossens</i>	
An Effective Placement of Detection Systems for Distributed Attack Detection in Large Scale Networks	204
<i>Seok Bong Jeong, Young Woo Choi, and Sehun Kim</i>	
Application of Content Computing in Honeyfarm	211
<i>Yi-Yuan Huang, Kwok-Yan Lam, Siu-Leung Chung, Chi-Hung Chi, and Jia-Guang Sun</i>	

Digital Rights Management

License Protection with a Tamper-Resistant Token	223
<i>Cheun Ngen Chong, Bin Ren, Jeroen Doumen, Sandro Etalle, Pieter H. Hartel, and Ricardo Corin</i>	
An Adaptive Approach to Hardware Alteration for Digital Rights Management	238
<i>Yinyan Yu and Zhi Tang</i>	
Dynamic Fingerprinting over Broadcast Using Revocation Scheme.....	251
<i>Mira Kim, Kazukuni Kobara, and Hideki Imai</i>	
Practical Pay-TV Scheme Using Traitor Tracing Scheme for Multiple Channels	264
<i>Chong Hee Kim, Yong Ho Hwang, and Pil Joong Lee</i>	

e-Commerce Security

- Vulnerability of a Mobile Payment System Proposed at WISA 2002 278
Sang Cheol Hwang, Dong Hoon Lee, Daewan Han, and Jae-Cheol Ryou
- Fair Offline Payment Using Verifiable Encryption 286
Sangjin Kim and Heekuck Oh
- A Limited-Use Key Generation Scheme for Internet Transactions..... 302
Supakorn Kungpisdan, Phu Dung Le, and Bala Srinivasan

Efficient Implementation

- Efficient Representation and Software Implementation
of Resilient Maiorana-McFarland S-boxes 317
Kishan Chand Gupta and Palash Sarkar
- Signed Digit Representation with NAF and Balanced Ternary Form
and Efficient Exponentiation in $GF(q^n)$
Using a Gaussian Normal Basis of Type II 332
Soonhak Kwon
- Novel Efficient Implementations of Hyperelliptic Curve Cryptosystems
Using Degenerate Divisors 345
*Masanobu Katagi, Izuru Kitamura, Toru Akishita,
and Tsuyoshi Takagi*
- Hyperelliptic Curve Coprocessors on a FPGA 360
*HoWon Kim, Thomas Wollinger, YongJe Choi, KyoIl Chung,
and Christof Paar*

Anonymous Communication

- Key-Exchange Protocol Using Pre-agreed Session-ID 375
Kenji Imamoto and Kouichi Sakurai
- A New k -Anonymous Message Transmission Protocol..... 388
Gang Yao and Dengguo Feng
- Onions Based on Universal Re-encryption –
Anonymous Communication Immune Against Repetitive Attack 400
Marcin Gomułkiewicz, Marek Klonowski, and Mirosław Kutylowski

Side-Channel Attacks

- Side Channel Cryptanalysis on SEED 411
*HyungSo Yoo, ChangKyun Kim, JaeCheol Ha, SangJae Moon,
and IlHwan Park*

XII Table of Contents

Secure and Efficient AES Software Implementation for Smart Cards	425
<i>Elena Trichina and Lesya Korkishko</i>	
Practical Template Attacks	440
<i>Christian Rechberger and Elisabeth Oswald</i>	
Evaluation and Improvement of the Tempest Fonts	457
<i>Hidema Tanaka, Osamu Takizawa, and Akihiro Yamamura</i>	
Author Index	471

Information Security Applications

5th International Workshop, WISA 2004, Jeju Island,
Korea, August 23-25, 2004, Revised Selected Papers

Lim, C.H.; Yung, M. (Eds.)

2005, XII, 472 p., Softcover

ISBN: 978-3-540-24015-0