# Table of Contents

## Public Key Crypto Applications/Virus Protection

Controllable Ring Signatures ............................................. 1  
*Wei Gao, Guilin Wang, Xueli Wang, and Dongqing Xie*

Efficient User Authentication and Key Agreement in Wireless Sensor Networks ......................................................... 15  
*Wen-Sheng Juang*

Identity-Based Key Issuing Without Secure Channel in a Broad Area ................................................................. 30  
*Saeran Kwon and Sang-Ho Lee*

PolyI-D: Polymorphic Worm Detection Based on Instruction Distribution .............................................................. 45  
*Ki Hun Lee, Yuna Kim, Sung Je Hong, and Jong Kim*

## Cyber Indication/Intrusion Detection

*Jianqing Ma, Shiyong Zhang, Yiping Zhong, and Xiaowen Tong*

SQL Injection Attack Detection: Profiling of Web Application Parameter Using the Sequence Pairwise Alignment .......................... 74  
*Jae-Chul Park and Bong-Nam Noh*

sIDMG: Small-Size Intrusion Detection Model Generation of Complimenting Decision Tree Classification Algorithm ...................... 83  
*Seung-Hyun Paek, Yoon-Keun Oh, and Do-Hoon Lee*

## Biometrics/Security Trust Management

Privacy-Enhancing Fingerprint Authentication Using Cancelable Templates with Passwords .................................................. 100  
*Daesung Moon, Sungju Lee, Seunghwan Jung, Youngwa Chung, Okyeon Yi, Namil Lee, and Kiyoung Moon*
<table>
<thead>
<tr>
<th>Topic</th>
<th>Title</th>
<th>Author(s)</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Impact of Embedding Scenarios on the Smart Card-Based Fingerprint Verification</td>
<td>Byungkwan Park, Daesung Moon, Yongwha Chung, and Jin-Won Park</td>
<td>110</td>
<td></td>
</tr>
<tr>
<td>Quality Assurance for Evidence Collection in Network Forensics</td>
<td>Bo-Chao Cheng and Huan Chen</td>
<td>121</td>
<td></td>
</tr>
<tr>
<td>Secure Software/Systems</td>
<td>Visualization of Permission Checks in Java Using Static Analysis</td>
<td>Yoonkyung Kim and Byeong-Mo Chang</td>
<td>133</td>
</tr>
<tr>
<td></td>
<td>Deployment of Virtual Machines in Lock-Keeper</td>
<td>Feng Cheng and Christoph Meinel</td>
<td>147</td>
</tr>
<tr>
<td>Smart Cards/Secure Hardware</td>
<td>Investigations of Power Analysis Attacks and Countermeasures for ARIA</td>
<td>HyungSo Yoo, Christoph Herbst, Stefan Mangard, Elisabeth Oswald, and SangJae Moon</td>
<td>160</td>
</tr>
<tr>
<td></td>
<td>A Novel Key Agreement Scheme in a Multiple Server Environment</td>
<td>Chin-Chen Chang and Chia-Chi Wu</td>
<td>187</td>
</tr>
<tr>
<td>Mobile Security</td>
<td>Cost-Effective IDS Operating Scheme in MANETs</td>
<td>Youngok Jeong, Younggoo Han, Hyunwoo Kim, Woochul Shim, Jaehong Kim, and Sehun Kim</td>
<td>198</td>
</tr>
<tr>
<td></td>
<td>Authenticated Fast Handover Scheme in the Hierarchical Mobile IPv6</td>
<td>Hyun-Sun Kang and Chang-Seop Park</td>
<td>211</td>
</tr>
<tr>
<td></td>
<td>A Method and Its Usability for User Authentication by Utilizing a Matrix Code Reader on Mobile Phones</td>
<td>Michiru Tanaka and Yoshimi Teshigawara</td>
<td>225</td>
</tr>
</tbody>
</table>
Table of Contents

DRM/Information Hiding/Ubiquitous Computing
Security/P2P Security

Distributed Management of OMA DRM Domains ........................................ 237
Harikrishna Vasanta, Reihaneh Safavi-Naini,
Nicholas Paul Sheppard, and Jan Martin Surminen

New Traceability Codes Against a Generalized Collusion Attack for
Digital Fingerprinting .............................................................................. 252
Hideki Yagi, Toshiyasu Matsushima, and Shigeichi Hirasawa

A Key Management Based on Multiple Regression in Hierarchical
Sensor Network ...................................................................................... 267
Mihui Kim, Inshil Doh, and Kijoon Chae

Random Visitor: A Defense Against Identity Attacks in P2P Overlay
Networks ............................................................................................... 282
Jabeom Gu, Jaehoon Nah, Cheoljoo Chae, Jaekwang Lee, and
Jongsoo Jang

Privacy/Anonymity

Privacy Protection in PKIs: A Separation-of-Authority Approach .......... 297
Taekyoung Kwon, Jung Hee Cheon, Yongdae Kim, and Jae-Il Lee

Three-Party Password Authenticated Key Agreement Resistant to
Server Compromise ................................................................................ 312
Taekyoung Kwon and Dong Hoon Lee

Privacy-Enhanced Content Distribution and Charging Scheme Using
Group Signature ...................................................................................... 324
Takayuki Tobita, Hironori Yamamoto, Hiroshi Doi, and
Keigo Majima

Secret Handshake with Multiple Groups ................................................. 339
Naoyuki Yamashita and Keisuke Tanaka

Internet and Wireless Security

Pre-authentication for Fast Handoff in Wireless Mesh Networks with
Mobile APs .............................................................................................. 349
Chanil Park, Junbeom Hur, Chanoe Kim, Young-joo Shin, and
Hyunsoo Yoon
EAP Using the Split Password-Based Authenticated Key Agreement ... 364
  Jongho Ryu

How Many Malicious Scanners Are in the Internet? ...................... 381
  Hiroaki Kikuchi and Masato Terada

E-Passport: The Global Traceability Or How to Feel Like a UPS Package... 391
  Dario Carluccio, Kerstin Lemke-Rust, Christof Paar, and
  Ahmad-Reza Sadeghi

Author Index ................................................................. 405