Information Security and Cryptology – ICISC 2003

6th International Conference
Seoul, Korea, November 27-28, 2003
Revised Papers
Preface

We would like to express a hearty welcome to all the participants of the 6th International Conference on Information Security and Cryptology (ICISC 2003). It was organized by the Korea Institute of Information Security and Cryptology (KIISC) and sponsored by the Korean Ministry of Information and Communication, and was held at the Seoul Olympic Parktel, Korea from November 27 to 28, 2003. As in the five previous years, it served as a forum to bring together researchers from academia and commercial developers from industry to discuss the current state of the art in information security and cryptology.

The Program Committee received 163 submissions from 25 countries and regions (Australia, Austria, Belgium, Canada, China, Finland, France, Germany, Hong Kong, India, Indonesia, Iran, Italy, Japan, Korea, Netherlands, Malaysia, Poland, Russia, Switzerland, Singapore, Taiwan, Turkey, UK, and USA), of which 32 papers were selected for presentation. All submissions were anonymously reviewed by at least 3 experts in the relevant areas. There were two invited talks, by Jonathan Katz and Jean-Jacques Quisquater.

We are very grateful to all the Program Committee members who devoted much effort and valuable time to reading and selecting the papers. We also thank the external experts who assisted the Program Committee in evaluating various papers. We owe special thanks to Jung Yeon Hwang and Judy Kang for always being available when their helping hand was needed.

Finally, we would like to thank all the authors who submitted papers to ICISC 2003, including those whose submissions were not successful, and the participants who together made this conference an intellectually stimulating event through their active contribution.

December 2003

Jong In Lim, Dong Hoon Lee
ICISC 2003

2003 International Conference on Information Security and Cryptology

Seoul Olympic Parktel, Seoul, Korea
November 27–28, 2003

Organized by

Korea Institute of Information Security and Cryptology (KIISC)
(http://www.kiisc.or.kr)

Sponsored by

MIC (Ministry of Information and Communication), Korea
(http://www.mic.go.kr)
Organization

General Chair
Se Hun Kim

Program Co-chairs
Jong In Lim
Dong Hoon Lee

Program Committee
Ronald Cramer
Zongduo Dai
Ed Dawson
Robert H. Deng
Jovan Golic
Gene Itkis
Markus Jakobsson
Kwangjo Kim
Pil Joong Lee
Seongan Lim
Masahiro Mambo
Sang Jae Moon
Chanathip Namprempre
David Naccache
Tatsuaki Okamoto
Choonsik Park
Dingyi Pei
David Pointcheval
Bart Preneel
Jean-Jacques Quisquater
Kouichi Sakurai
Palash Sarkar
Nigel Smart
Serge Vaudenay
Sung-Ming Yen
Moti Yung

KAIST, Korea
Korea University, Korea
Aarhus, Denmark
Academia Sinica, China
Queensland University of Technology, Australia
Institute for Infocomm Research, Singapore
Tilab, Telecom Italia, Italy
Boston University, USA
RSA Laboratories, USA
ICU, Korea
POSTECH, Korea
Korea Information Security Agency, Korea
Tohoku University, Japan
Thammasat University, Thailand
Gemplus Card International, France
NTT, Japan
ETRI, Korea
Chinese Academy of Science, China
CNRS/ENS, France
Katholieke Universiteit Leuven, Belgium
UCL, Belgium
Kyushu University, Japan
Indian Statistical Institute, India
University of Bristol, UK
EPFL, Switzerland
National Central University, Taiwan
Columbia University, USA
Organizing Committee Chair

Heung Youl Youm
Soonchunhyang University, Korea

Organizing Committee

HaGwang Soo Rhee
Ji Hong Kim
Kyo Il Chung
Jae Cheol Ha
Hong Geun Kim
Su Kyung Chae
Kyung Sim Kim
Sookmyung Women’s University, Korea
Semyung University, Korea
ETRI, Korea
Korea Nazarene University, Korea
KISA, Korea
MIC, Korea
KIISC, Korea

External Reviewers

Alex Biryukov
Alex Dent
Andrew Clark
Beatrice Peirani
Bo-Ching Wu
Chang Seop Park
Chao-Chih Hsu
Chi-Dian Wu
Chien-ning Chen
Chong Hee Kim
Christophe De Canniere
Claude Barral
Dae Hyun Yum
Dan Page
Dario Catalano
Dingyi Pei
Dong Jin PARK
Emmanuel Bresson
Eric Brier
E-Transaction Protection Tech team
Eul Gyu Im
Frederik Vercauteren
G. Hanaoka
Geriant Price
Gildas Avoine
Gregory Neven
Guohua Xiong
Helena Handschuh
Helger Lipmaa

Henry Lee
Hisashi Inoue
Hsi-Chung Lin
Huafei Zhu
Hyeong Joon Kim
Hyeong Joong Kim
In Kook Park
Jacques Fournier
Jae Hwan Park
Javier Herranz Sotoca
Javier Herranz Sotoca
Jean Monnerat
Jean Sebastien Coron
Jean-Francois Dhem
Ji Hyun Jeong
John Malone-Lee
Jonghoon Shin
Joon-Hah Park
Joseph Lano
Juanma Gonzalez-Nieto
Julien Brouchier
JuSung Kang
Katsu Okeya
Kazu Fukushima
Kazuto Matsuo
Kenji Imamoto
Ki Sik Chang
Kishan Chand Gupta
Kun Peng
## Table of Contents

### Invited Talk

Binary Tree Encryption: Constructions and Applications  
*Jonathan Katz* .......................................................... 1

### Digital Signatures I

A Separable Threshold Ring Signature Scheme  
*Joseph K. Liu, Victor K. Wei, and Duncan S. Wong* .............. 12

On the Security of a Group Signature Scheme with Forward Security  
*Guilin Wang* .......................................................... 27

An Efficient Strong Designated Verifier Signature Scheme  
*Shahrokh Saeednia, Steve Kremer, and Olivier Markowitch* ........ 40

### Primitives

Sound Computational Interpretation of Formal Encryption with Composed Keys  
*Peeter Laud and Ricardo Corin* ........................................ 55

On the Security of a New Variant of OMAC  
*Tetsu Iwata and Kaoru Kurosawa* .................................... 67

New Methods to Construct Cheating Immune Functions  
*Wen Ping Ma and Moon Ho Lee* .................................... 79

Yet Another Definition of Weak Collision Resistance and Its Analysis  
*Shoichi Hirose* ........................................................... 87

### Fast Implementations

Implementation of Tate Pairing on Hyperelliptic Curves of Genus 2  
*YoungJu Choie and Eunjeong Lee* .................................... 97

A General Expansion Method Using Efficient Endomorphisms  
*Tae-Jun Park, Mun-Kyu Lee, E-yong Kim, and Kunsoo Park* ........ 112
| Design of Bit Parallel Multiplier with Lower Time Complexity | Seon Ok Lee, Seok Won Jung, Chang Han Kim, Janghong Yoon, Jae-Young Koh, and Daeho Kim | 127 |
| Architecture for an Elliptic Curve Scalar Multiplication Resistant to Some Side-Channel Attacks | Joong Chul Yoon, Seok Won Jung, and Sungwoo Lee | 139 |
| Efficient Scalar Multiplication in Hyperelliptic Curves Using A New Frobenius Expansion | Tae-Jun Park, Mun-Kyu Lee, and Kunsoo Park | 152 |

**Computer Security/Mobile Security**

Adaptive Protocol for Entity Authentication and Key Agreement in Mobile Networks | Muxiang Zhang | 166 |

Extended Role Based Access Control and Procedural Restrictions | Wook Shin, Dong-Ik Lee, Hyoung-Chun Kim, Jung-Min Kang, and Jin-Seok Lee | 184 |

Layer-Based Access Control Model in the Manufacturing Infrastructure and Design Automation System | Yuan Zhang, Moon Jung Chung, and Hyun Kim | 197 |

**Voting/Auction Protocols**

Secure Double Auction Protocols with Full Privacy Protection | Changjie Wang, Ho-fung Leung, and Yumin Wang | 215 |

Sealed-Bid Auctions with Efficient Bids | Toru Nakanishi, Daisuke Yamamoto, and Yuji Sugiyama | 230 |

Providing Receipt-Freeness in Mixnet-Based Voting Protocols | Byoungcheon Lee, Colin Boyd, Ed Dawson, Kwangjo Kim, Jeongmo Yang, and Seungjae Yoo | 245 |

Receipt-Free Electronic Auction Schemes Using Homomorphhic Encryption | Xiaofeng Chen, Byoungcheon Lee, and Kwangjo Kim | 259 |

**Watermarking**

Software Watermarking Through Register Allocation: Implementation, Analysis, and Attacks | Ginger Myles and Christian Collberg | 274 |

Analysis of the Bounds for Linear Block Codes in Watermark Channel | Limin Gu, Jiwu Huang, and Zewen Chen | 294 |
Digital Signatures II

Security Analysis of Some Proxy Signatures
Guilin Wang, Feng Bao, Jianying Zhou, and Robert H. Deng ............ 305

A More Secure and Efficacious TTS Signature Scheme
Jiun-Ming Chen and Bo-Yin Yang ........................................ 320

An Efficient Revocation Algorithm in Group Signatures
Zewen Chen, Jilin Wang, Yumin Wang, Jiwu Huang, and Daren Huang .. 339

Efficient Forward and Provably Secure ID-Based Signcryption Scheme
with Public Verifiability and Public Ciphertext Authenticity
Sherman S.M. Chow, S.M. Yiu, Lucas C.K. Hui, and K.P. Chow ......... 352

Authentication/Threshold Protocols

Group Oriented Cryptosystems Based on Linear Access Structures
Wen Ping Ma and Moon Ho Lee ............................................ 370

A New Algorithm for Searching a Consistent Set of Shares
in a Threshold Scheme with Cheaters
Raylin Tso, Ying Miao, and Eiji Okamoto .................................. 377

Non-interactive Deniable Ring Authentication
Willy Susilo and Yi Mu ..................................................... 386

Block/Stream Ciphers

Differential Cryptanalysis of TEA and XTEA
Seokhie Hong, Deukjo Hong, Youngdai Ko, Donghoon Chang,
Wonil Lee, and Sangjin Lee .............................................. 402

A Complete Divide and Conquer Attack on the Alpha1 Stream Cipher

New Block Cipher: ARIA
Daesung Kwon, Jaesung Kim, Sangwoo Park, Soo Hak Sung,
Yaekwon Sohn, Junghwan Song, Yongjin Yeom, E-joong Yoon,
Sangjin Lee, Jaewon Lee, Seongtaek Chee, Daewan Han, and Jin Hong ... 432

Truncated Differential Attacks on 8-Round CRYPTON
Jongsung Kim, Seokhie Hong, Sangjin Lee, Junghwan Song,
and Hyungjin Yang ......................................................... 446

Author Index ............................................................... 457