

Commenced Publication in 1973

Founding and Former Series Editors:

Gerhard Goos, Juris Hartmanis, and Jan van Leeuwen

Editorial Board

David Hutchison

Lancaster University, UK

Takeo Kanade

Carnegie Mellon University, Pittsburgh, PA, USA

Josef Kittler

University of Surrey, Guildford, UK

Jon M. Kleinberg

Cornell University, Ithaca, NY, USA

Friedemann Mattern

ETH Zurich, Switzerland

John C. Mitchell

Stanford University, CA, USA

Moni Naor

Weizmann Institute of Science, Rehovot, Israel

Oscar Nierstrasz

University of Bern, Switzerland

C. Pandu Rangan

Indian Institute of Technology, Madras, India

Bernhard Steffen

University of Dortmund, Germany

Madhu Sudan

Massachusetts Institute of Technology, MA, USA

Demetri Terzopoulos

University of California, Los Angeles, CA, USA

Doug Tygar

University of California, Berkeley, CA, USA

Moshe Y. Vardi

Rice University, Houston, TX, USA

Gerhard Weikum

Max-Planck Institute of Computer Science, Saarbruecken, Germany

Min Surp Rhee Byoungcheon Lee (Eds.)

Information Security and Cryptology – ICISC 2006

9th International Conference
Busan, Korea, November 30 - December 1, 2006
Proceedings

Volume Editors

Min Surp Rhee
Dankook University
San 29, Anseo-dong, Cheonan-shi
Chungnam, 330-714, Korea
E-mail: msrhee@dankook.ac.kr

Byoungcheon Lee
Joongbu University
101 Daehak-Ro, Chubu-Myeon, Guemsan-Gun
Chungnam, 312-702, Korea
E-mail: sultan@joongbu.ac.kr

Library of Congress Control Number: 2006936103

CR Subject Classification (1998): E.3, G.2.1, D.4.6, K.6.5, F.2.1, C.2, J.1

LNCS Sublibrary: SL 4 – Security and Cryptology

ISSN 0302-9743
ISBN-10 3-540-49112-0 Springer Berlin Heidelberg New York
ISBN-13 978-3-540-49112-5 Springer Berlin Heidelberg New York

This work is subject to copyright. All rights are reserved, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, re-use of illustrations, recitation, broadcasting, reproduction on microfilms or in any other way, and storage in data banks. Duplication of this publication or parts thereof is permitted only under the provisions of the German Copyright Law of September 9, 1965, in its current version, and permission for use must always be obtained from Springer. Violations are liable to prosecution under the German Copyright Law.

Springer is a part of Springer Science+Business Media
springer.com

© Springer-Verlag Berlin Heidelberg 2006
Printed in Germany

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India
Printed on acid-free paper SPIN: 11927587 06/3142 5 4 3 2 1 0

Preface

ICISC 2006, the Ninth International Conference on Information Security and Cryptology, was held in Busan, Korea, during November 30 - December 1, 2006. It was organized by the Korea Institute of Information Security and Cryptology (KIISC) in cooperation with the Ministry of Information and Communication (MIC), Korea. The aim of this conference was to provide a forum for the presentation of new results in research, development, and application in information security and cryptology. It also intended to be a place where research information can be exchanged.

Started in 1998, ICISC has grown into an important international conference in the information security and cryptology area with an established reputation. Based on this maturity, we tried an important change in the publication policy this year. Until last year, pre-proceedings were distributed at the conference and proceedings in Springer's *Lecture Notes in Computer Science* (LNCS) were published after the conference. This year ICISC proceedings were published in LNCS before the conference and distributed to the participants at the conference. We appreciate Springer for their full support and help in making this possible.

The conference received 129 submissions from 17 countries, covering all areas of information security and cryptology. The review and selection processes were carried out in two stages by the Program Committee of 57 prominent researchers via online meetings through the iChair Web server. First, each paper was blind reviewed by at least three PC members, and papers co-authored by the PC members were reviewed by at least five PC members. Second, individual review reports were revealed to PC members, and detailed interactive discussion on each paper followed. Through this process the Program Committee finally selected 26 papers from 12 countries. The authors of selected papers had a few weeks to prepare final versions of their papers, aided by comments from the reviewers. The proceedings contain the revised versions of the accepted papers. However, most of these final revisions were not subject to any further editorial review.

The conference program included two invited talks from eminent researchers in information security and cryptology. Serge Vaudenay from EPFL gave an interesting talk on RFID privacy entitled "RFID Privacy Based on Public-Key Cryptography." Palash Sarkar from the Indian Statistical Institute talked on "Generic Attacks on Symmetric Ciphers," which showed various time-memory trade-off attacks on symmetric cipher algorithms.

We would like to thank everyone who contributed to the success of this conference. First, thanks to all the authors who submitted papers to this conference. Second, thanks to all 57 members of the Program Committee listed overleaf. It was a truly nice experience to work with such talented and hard-working researchers. Third, thanks to all the external reviewers for assisting the Program Committee in their particular areas of expertise. Fourth, we would like to thank

all the participants of the event who made this event an intellectually stimulating one through their active contribution. We also would like to thank the iChair developers in EPFL for allowing us to use their software. Finally, we are delighted to acknowledge the partial financial support provided by Redgate, SECUi.COM, MarkAny, and EK Manpower.

November 2006

Min Surp Rhee
Byoungcheon Lee

Organization

General Chair

JooSeok Song Yonsei University, Korea

Program Co-chairs

Min Surp Rhee Dankook University, Korea
Byoungcheon Lee Joongbu University, Korea

Program Committee

Giuseppe Ateniese The Johns Hopkins University, USA
Joonsang Baek Institute for Infocomm Research, Singapore
Alex Biryukov University of Luxembourg, Luxembourg
John Black University of Colorado, USA
Jean-Sebastien Coron University of Luxembourg, Luxembourg
Jung Hee Cheon Seoul National University, Korea
Kyo-il Chung ETRI, Korea
Ed Dawson Queensland University of Technology, Australia
Yevgeniy Dodis New York University, USA
Serge Fehr CWI Amsterdam, Netherlands
Pierre-Alain Fouque Ecole Normale Supérieure, France
Marc Girault France Telecom, France
Philippe Golle Palo Alto Research Center, USA
Dieter Gollmann Hamburg University of Technology, Germany
Yongfei Han ONETS, China
Goichiro Hanaoka AIST, Japan
Marc Joye Gemplus, France
Jonathan Katz University of Maryland, USA
Hiroaki Kikuchi Tokai University, Japan
Hwankoo Kim Hoseo University, Korea
Kwangjo Kim ICU, Korea
Kaoru Kurosawa Ibaraki University, Japan
Taekyoung Kwon Sejong University, Korea
Chi Sung Laih Kun Shan University, Taiwan
Kwok-Yan Lam Tsinghua University, China
Dong Hoon Lee Korea University, Korea
Pil Joong Lee POSTECH, Korea
Sang-Ho Lee Ewha Womans University, Korea
Arjen Lenstra EPFL, Switzerland
Yingjiu Li Singapore Management University, Singapore

| | |
|------------------------|--|
| Helger Lipmaa | Cybernetica AS and University of Tartu, Estonia |
| Javier Lopez | University of Malaga, Spain |
| Masahiro Mambo | University of Tsukuba, Japan |
| Keith Martin | Royal Holloway, University of London, UK |
| Mitsuru Matsui | Mitsubishi Electric Corporation, Japan |
| Chris Mitchell | Royal Holloway, University of London, UK |
| Atsuko Miyaji | JAIST, Japan |
| SangJae Moon | Kyungpook National University, Korea |
| Yi Mu | University of Wollongong, Australia |
| Rei Safavi-Naini | Wollongong University, Australia |
| Jesper Buus Nielsen | Aarhus University, Denmark |
| DaeHun Nyang | Inha University, Korea |
| Rolf Oppliger | eSECURITY Technologies, Switzerland |
| Carles Padro | Technical University of Catalonia, Spain |
| Raphael Chung-Wei Phan | Swinburne University of Technology, Malaysia |
| Kouichi Sakurai | Kyushu University, Japan |
| Palash Sarkar | Indian Statistical Institute, India |
| Nigel Smart | University of Bristol, UK |
| Willy Susilo | University of Wollongong, Australia |
| Tsuyoshi Takagi | Future University - Hakodate, Japan |
| Serge Vaudenay | EPFL, Switzerland |
| Guilin Wang | Institute for Infocomm Research, Singapore |
| William Whyte | NTRU Cryptosystems, USA |
| Michael Wiener | Cryptographic Clarity, Canada |
| Dongho Won | Sungkyunkwan University, Korea |
| Sung-Ming Yen | National Central University, Taiwan |
| Yongjin Yeom | NSRI, Korea |
| Fangguo Zhang | Sun Yat-sen University, China |
| Alf Zugenmaier | DoCoMo Euro-Labs, Germany |

Organizing Chair

| | |
|------------------|------------------------------------|
| Kyung-Hyune Rhee | Pukyong National University, Korea |
|------------------|------------------------------------|

Organizing Committee

| | |
|---------------|------------------------------------|
| Chang Kyu Kim | Dong-eui University, Korea |
| Heekuck Oh | Hanyang University, Korea |
| Im-Yeong Lee | Soonchunhyang University, Korea |
| Sang-Uk Shin | Pukyong National University, Korea |
| Weon Shin | Tongmyong University, Korea |
| HoonJae Lee | Dongseo University, Korea |
| Dong Kyue Kim | Hanyang University, Korea |

External Reviewers

| | | |
|-------------------|---------------------|----------------------|
| Imad Aad | Ik rae Jeong | Jung Hyung Park |
| Imad Abbadi | Seny Kamara | Sangjoon Park |
| Michelle Abdalla | Jeonil Kang | Tae Jun Park |
| Toru Akishita | Eike Kiltz | Sylvain Pasini |
| Patrick Amon | Hyung Chan Kim | Geong Sen Poh |
| Thomas Baigneres | Jonghyun Kim | Rodrigo Roman |
| Simon Blackburn | Tae Hyun Kim | Louis Salvail |
| Marina Blanton | Youngsoo Kim | Farzad Salim |
| Brian Carrier | Shinsaku Kiyomoto | Christian Schaefer |
| Michael Cheng | Tetsutaro Kobayashi | Jae Woo Seo |
| Sangrae Cho | Divyan M. Konidala | Nicholas Sheppard |
| Seokhyang Cho | Noboru Kunihiro | Jong Hoon Shin |
| Yong-Je Choi | Nam-Suk Kwarac | SeongHan Shin |
| Sherman Chow | Sven Lachmund | Douglas Sicker |
| Andrew Clark | Julien Laganier | Hongwei Sun |
| Yang Cui | Vinh The Lam | Clark Thomborson |
| John Daugman | HoonJae Lee | Dongvu Tonien |
| Alain Durand | Jin Li | Eran Tromer |
| Andrzej Drygajlo | Wanqing Li | Yoshifumi Ueshige |
| Dang Nguyen Duc | Hsi-Chung Lin | Masashi Une |
| Gerardo Fernandez | JongHyup Lee | Frederik Vercauteren |
| Matthieu Finiasz | MunKyu Lee | Duc Liem Vo |
| Aline Gouget | Soo-hyung Lee | Martin Vuagnoux |
| Matthew Green | Yunho Lee | Camille Vuillaume |
| JaeCheol Ha | Jiqiang Lu | Thomas Walter |
| Genebeck Hahn | Liang Lu | Baodian Wei |
| Javier Herranz | Tal Malkin | Chung-Huang Yang |
| Susan Hohenberger | Kanta Matsuura | Yeon Hyeong Yang |
| Jungdae Hong | Breno de Medeiros | Eunsun Yoo |
| Yoshiaki Hori | Kunihiko Miyazaki | Sung-Soo Yoon |
| Jeffrey Horton | George Mohay | Dae Hyun Yum |
| Xinyi Huang | Jean Monnerat | Rui Zhang |
| John Ioannidis | Dae Sung Moon | Chang'an Zhao |
| Toshiyuki Isshiki | Kazuto Ogawa | Sebastien Zimmer |
| Tetsuya Izu | Takeshi Okamoto | |
| Jingak Jang | Dan Page | |

Sponsoring Institutions

| | |
|--------------------|---|
| Redgate, Korea | http://www.redgate.co.kr/ |
| SECUI.COM, Korea | http://www.secui.com/ |
| MarkAny, Korea | http://www.markany.com/ |
| EK Manpower, Korea | http://www.ekmanpower.co.kr/ |

Table of Contents

Invited Talks

| | |
|---|---|
| RFID Privacy Based on Public-Key Cryptography | 1 |
| <i>Serge Vaudenay</i> | |
| Generic Attacks on Symmetric Ciphers | 7 |
| <i>Palash Sarkar</i> | |

Hash Functions – I

| | |
|--|----|
| Improved Collision Attack on the Hash Function Proposed at PKC'98 | 8 |
| <i>Florian Mendel, Norbert Pramstaller, Christian Rechberger</i> | |
| Hashing with Polynomials | 22 |
| <i>Vladimir Shpilrain</i> | |
| Birthday Paradox for Multi-collisions | 29 |
| <i>Kazuhiro Suzuki, Dongvu Tonien, Kaoru Kurosawa, Koji Toyota</i> | |

Block and Stream Ciphers

| | |
|--|----|
| New Variant of the Self-Shrinking Generator and Its Cryptographic Properties | 41 |
| <i>Ku-Young Chang, Ju-Sung Kang, Mun-Kyu Lee, Hangrok Lee, Downon Hong</i> | |
| On Constructing of a 32×32 Binary Matrix as a Diffusion Layer for a 256-Bit Block Cipher | 51 |
| <i>Bon Wook Koo, Hwan Seok Jang, Jung Hwan Song</i> | |
| On Algebraic Immunity and Annihilators | 65 |
| <i>Xian-Mo Zhang, Josef Pieprzyk, Yuliang Zheng</i> | |

Efficient Implementation and Hardware

| | |
|--|----|
| High-Speed RSA Crypto-processor with Radix-4 Modular Multiplication and Chinese Remainder Theorem | 81 |
| <i>Bonseok Koo, Dongwook Lee, Gwonho Ryu, Taejoo Chang, Sangjin Lee</i> | |

A High-Speed Square Root Algorithm in Extension Fields 94
*Hidehiro Katou, Feng Wang, Yasuyuki Nogami,
Yoshitaka Morikawa*

The Smallest ARIA Module with 16-Bit Architecture 107
Sangwoon Yang, Jinsub Park, Younggap You

A Simpler Sieving Device: Combining ECM and TWIRL 118
*Willi Geiselmann, Fabian Januszewski, Hubert Köpfer, Jan Pelzl,
Rainer Steinwandt*

Network Security and Access Control

Janus: A Two-Sided Analytical Model for Multi-Stage
Coordinated Attacks 136
Zonghua Zhang, Pin-Han Ho, Xiaodong Lin, Hong Shen

A Time-Frame Based Trust Model for P2P Systems 155
Junsheng Chang, Huaimin Wang, Gang Yin

Spatial Context in Role-Based Access Control 166
Hong Zhang, Yeping He, Zhiguo Shi

Mobile Communications Security

An Efficient Scheme for Detecting Malicious Nodes in Mobile
Ad Hoc Networks 179
Jongoh Choi, Si-Ho Cha, JooSeok Song

Mobile RFID Applications and Security Challenges 194
Divyan M. Konidala, Kwangjo Kim

Forensics

An Efficient Forensic Evidence Collection Scheme of Host
Infringement at the Occurrence Time 206
*Yoon-Ho Choi, Jong-Ho Park, Sang-Kon Kim, Seung-Woo Seo,
Yu Kang, Jin-Gi Choe, Ho-Kun Moon, Myung-Soo Rhee*

Copyright Protection

A Copy Protection Technique Using Multi-level
Error Coding 222
Chen-Yin Liao, Jen-Wei Yeh, Ming-Seng Kao

| | |
|---|-----|
| Digital Rights Management with Right Delegation for Home Networks | 233 |
| <i>Heeyoul Kim, Younho Lee, Byungchun Chung, Hyunsoo Yoon, Jaewon Lee, KyungIm Jung</i> | |

Biometrics

| | |
|---|-----|
| Fake Iris Detection Based on Multiple Wavelet Filters and Hierarchical SVM | 246 |
| <i>Kang Ryoung Park, Min Cheol Whang, Joa Sang Lim, Yongjoo Cho</i> | |

Hash Functions – II

| | |
|---|-----|
| Multi-block Collisions in Hash Functions Based on 3C and 3C+ Enhancements of the Merkle-Damgård Construction | 257 |
| <i>Daniel Joščák, Jiří Tůma</i> | |

| | |
|---|-----|
| Cryptanalysis of T-Function-Based Hash Functions Applications to MySQL Password Algorithms | 267 |
| <i>Frédéric Muller, Thomas Peyrin</i> | |

| | |
|---|-----|
| Collision Search Attack for 53-Step HAS-160 | 286 |
| <i>Hong-Su Cho, Sangwoo Park, Soo Hak Sung, Aaram Yun</i> | |

Public Key Cryptosystems

| | |
|--|-----|
| Klein Bottle Routing: An Alternative to Onion Routing and Mix Network | 296 |
| <i>Kun Peng, Juan Manuel Nieto, Yvo Desmedt, Ed Dawson</i> | |

| | |
|---|-----|
| New Constructions of Constant Size Ciphertext HIBE Without Random Oracle | 310 |
| <i>Sanjit Chatterjee, Palash Sarkar</i> | |

Digital Signatures

| | |
|--|-----|
| A New Proxy Signature Scheme Providing Self-delegation | 328 |
| <i>Younho Lee, Heeyoul Kim, Yongsu Park, Hyunsoo Yoon</i> | |

| | |
|---|-----|
| Extended Sanitizable Signatures | 343 |
| <i>Marek Klonowski, Anna Lauks</i> | |

| | |
|-------------------------------|------------|
| Author Index | 357 |
|-------------------------------|------------|