

*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*

Alfred Kobsa

*University of California, Irvine, CA, 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*

Gerhard Weikum

*Max-Planck Institute of Computer Science, Saarbruecken, Germany*

Pil Joong Lee Jung Hee Cheon (Eds.)

# Information Security and Cryptology – ICISC 2008

11th International Conference  
Seoul, Korea, December 3-5, 2008  
Revised Selected Papers

Volume Editors

Pil Joong Lee

Pohang University of Science and Technology (POSTECH)

Department of Electronic and Electrical Engineering

San 31 Hyoja-dong, Nam-gu, Pohang, Kyungbuk 790-784, Korea

E-mail: pjl@postech.ac.kr

Jung Hee Cheon

Seoul National University, Department of Mathematical Sciences

599 Gwanakno, Gwanak-gu, Seoul 151-742, Korea

E-mail: jhcheon@snu.ac.kr

Library of Congress Control Number: Applied for

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 3-642-00729-5 Springer Berlin Heidelberg New York

ISBN-13 978-3-642-00729-3 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.com

© Springer-Verlag Berlin Heidelberg 2009

Printed in Germany

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India

Printed on acid-free paper SPIN: 12631810 06/3180 5 4 3 2 1 0

# Preface

ICISC 2008, the 11th International Conference on Information Security and Cryptology, was held in Seoul, Korea, during December 3–5, 2008. It was organized by the Korea Institute of Information Security and Cryptology (KIISC). The aim of this conference was to provide a forum for the presentation of new results in research, development, and applications in the field of information security and cryptology. It also served as a place for research information exchange.

The conference received 131 submissions from 28 countries, covering all areas of information security and cryptology. The review and selection processes were carried out in two stages by the Program Committee (PC) of 62 prominent researchers via online meetings, using the We-Submission-and-Review software written by Shai Halevi, IBM. First, at least three PC members blind-reviewed each paper, 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, followed by detailed interactive discussion on each paper. Through this process, the PC finally selected 26 papers from 14 countries. The acceptance rate was 19.8%. The authors of selected papers had a few weeks to prepare for their final versions based on the comments received from more than 136 external reviewers. These revised papers were not subject to editorial review and the authors bear full responsibility for their contents.

The conference featured one tutorial and two invited talks. The tutorial was given by Masayuki Abe from NTT. The invited speakers for two talks were Vincent Rijmen from K.U.L. & Graz University of Tech and Jong-Deok Choi from Samsung Electronics.

There are many people who contributed to the success of ICISC 2008. We would like to thank all the authors who submitted papers to this conference. We are deeply grateful to all 62 members of the PC members. It was a truly nice experience to work with such talented and hard-working researchers. We wish to thank all the external reviewers for assisting the PC in their particular areas of expertise. Thanks to Shai Halevi for allowing us to use their convenient software. Finally, we would like to thank all the participants of the conference who made this event an intellectually stimulating one through their active contribution.

December 2008

Pil Joong Lee  
Jung Hee Cheon

# ICISC 2008

The 11th Annual International Conference  
on Information Security

December 3–5, 2008  
Sungkyunkwan University, Seoul, Korea

*Organized by*  
Korea Institute of Information Security and Cryptology (KIISC)  
<http://www.kiisc.or.kr>

*In cooperation with*  
Ministry of Knowledge Economy (MKE)  
<http://www.mke.go.kr>

## General Chair

Hong-sub Lee                      KIISC, Korea

## Program Co-chairs

Pil Joong Lee                      POSTECH, Korea  
Jung Hee Cheon                    Seoul National University, Korea

## Program Committee

Joonsang Baek	Institute for Infocomm Research, Singapore
Liqun Chen	Hewlett-Packard Laboratories, UK
Nicolas T. Courtois	University College London, UK
Michel Cukier	University of Maryland, USA
Frederic Cuppens	Telecom Bretagne, France
Bart De Decker	Katholieke Universiteit Leuven, Belgium
Mario Marques Freire	University of Beira Interior, Portugal
Philippe Golle	Palo Alto Research Center, USA
Guang Gong	University of Waterloo, Canada
Vipul Goyal	UCLA, USA
Kil-Chan Ha	Sejong University, Korea
Eduardo B. Fernandez	Florida Atlantic University, USA
Dowon Hong	ETRI, Korea
Jin Hong	Seoul National University, Korea
Seokhie Hong	Korea University, Korea
Stanislaw Jarecki	University of California, Irvine, USA
Jaeyeon Jung	Intel Research, USA

Kwangjo Kim	ICU, Korea
Yongdae Kim	University of Minnesota, Twin Cities, USA
Christopher Kruegel	University of California, Santa Barbara, USA
Taekyoung Kwon	Sejong University, Korea
Byoungcheon Lee	Joongbu University, Korea
Dong Hoon Lee	Korea University, Korea
Mun-Kyu Lee	Inha University, Korea
Yingjiu Li	Singapore Management University, Singapore
Chae Hoon Lim	Sejong University, Korea
Javier Lopez	University of Malaga, Spain
Keith Martin	Royal Holloway, University of London, UK
Sjouke Mauw	University of Luxembourg, Luxembourg
Atsuko Miyaji	JAIST, Japan
SangJae Moon	Kyungpook National University, Korea
David Naccache	Ecole Normale Superieure, France
Jesper Buus Nielsen	Aarhus University, Denmark
DaeHun Nyang	Inha University, Korea
Tatsuaki Okamoto	NTT, Japan
Rolf Oppliger	eSECURITY Technologies, Switzerland
Paolo D'Arco	University of Salerno, Italy
Je Hong Park	ETRI, Korea
Sangjoon Park	Sungkyunkwan University, Korea
Sangwoo Park	ETRI, Korea
Jacques Patarin	Versailles University, France
Raphael C.-W. Phan	Loughborough University, UK
Bart Preneel	Katholieke Universiteit Leuven, Belgium
Jean-Jacques Quisquater	UCL, Belgium
Vincent Rijmen	K.U.L., Belgium and Graz University of Technology, Austria
Ahmad-Reza Sadeghi	Ruhr University Bochum, Germany
Kouichi Sakurai	Kyushu University, Japan
Mahmoud Salmasizadeh	Sharif University of Technology, Iran
Palash Sarkar	Indian Statistical Institute, India
JungHwan Song	Hanyang University, Korea
Rainer Steinwandt	Florida Atlantic University, USA
Willy Susilo	University of Wollongong, Australia
Tsuyoshi Takagi	Future University Hakodate, Japan
Yukiyasu Tsunoo	NEC Corporation, Japan
Jozef Vyskoc	VaF s.r.o., Slovakia
Sung-Ming Yen	National Central University, Taiwan
Jeong Hyun Yi	Samsung, Korea
Hyunsoo Yoon	KAIST, Korea
Dae Hyun Yum	POSTECH, Korea
Moti Yung	Google Inc. and Columbia University, USA
Fangguo Zhang	Google Inc. and Columbia University, USA
Alf Zugenmaier	DoCoMo Euro-Labs, Germany

## Organizing Chair

Seungjoo Kim                      Sungkyunkwan University, Korea

## Organizing Committee

Dong Kyue Kim	Hanyang University, Korea
Ki Young Moon	ETRI, Korea
Chang-Seop Park	Dankook University, Korea
Young Ik Eom	Sungkyunkwan University, Korea
Heekuck Oh	Hanyang University, Korea
Dong Hoon Lee	Korea University, Korea
Im-Yeong Lee	Soonchunhyang University, Korea

## External Reviewers

Frederik Armknecht	Ton van Deursen	Divyan M. Konidala
Maryam Rajabzadeh	Gwenael Doerr	Heejin Park
Assar	Dang Nguyen Duc	Hiroyasu Kubo
Man Ho Au	Thomas Eisenbarth	Jeong Ok Kwon
Jean-Philippe Aumasson	Yehia Elrakaiby	Jorn Lapon
Fabien Autrel	Jonathan Etrog	HoonJae Lee
Behnam Bahrak	Kazuhide Fukushima	Ji-Seon Lee
Shane Balfe	Xinxin Fan	JongHyup Lee
Lejla Batina	Joaquin Garcia-Alfaro	Jun Ho Lee
Aurelie Bauer	Benedikt Gierlichs	Jung-Keun Lee
Robin Berthier	Henri Gilbert	Kwangsu Lee
Jean-Luc Beuchet	Yoshiaki Hori	Minsoo Lee
Annalisa De Bonis	JaeCheul Ha	Youngsook Lee
Antoon Bosselaers	Daewan Han	Jin Li
Yacine Bouzida	Honggang Hu	Wei-Chih Lien
Wouter Castryck	Xinyi Huang	Hsi-Chung Lin
Dario Catalano	Junbeom Hur	Kuan-Jen Lin
Donghoon Chang	Jung Yeon Hwang	Hans Loehr
Ku Young Chang	Sebastiaan Indesteege	Carolin Lunemann
Byong-Deok Choi	Hoda Jannati	Florian Mendel
Jae Tark Choi	Keith Jarrin	Hideyuki Miyake
Jeong Woon Choi	Ikrae, Jeong	Abedelaziz Mohaisen
Sherman Chow	Nam-su Jho	Amir Moradi
Danielle Chrun	Takeshi Kawabata	Tomislav Nad
Carlos Cid	Chano Kim	Vincent Naessens
Ed Condon	Jihye Kim	Akira Nozawa
Nora Cuppens-Boulahia	Jongsung Kim	Satoshi Obana
M. Prem Laxman Das	Takayuki Kimura	Chihiro Ohyama

Katsuyuki Okeya	Teruo Saito	Pieter Verhaeghe
Claudio Orlandi	Somitra Kumar	Ivan Visconti
Kyosuke Osaka	Sanadhya	Camille Vuillaume
Omkant Pandey	Riccardo Scandariato	Christian Wachsmann
Jun Pang	Martin Schläffer	Yamin Wen
Chanil Park	Jae Woo Seo	Jian Weng
Hyun-A Park	Maki Shigeri	Bo-Ching Wu
YongSu Park	Masaaki Shirase	Chi-Dian Wu
Young-Ho Park	Haya Shulman	Lingling Xu
Axel Poschmann	Masakazu Soshi	OkYeon Yi
Roberto De Prisco	Miroslava Sotakova	Yves Younan
Sasa Radomirovic	Takahiko Syouji	Ng Ching Yu
Christian Rechberger	Tamer	Aaram Yun
Mohammad Reza	Julien Thomas	Chang-An Zhao
Reyhaniatabar	Joe-Kai Tsay	Xingwen Zhao
Chunhua Su	Etsuko Tsujihara	Tieyan Li
Minoru Saeki	Frederik Vercauteren	

## Sponsoring Institutions

BCQRE

Chungnam National University Internet Intrusion Response Technology

Research Center (CNU IIRTRC), Korea

Electronics and Telecommunications Research Institute (ETRI), Korea

IglooSecurity, Korea

Korea Electronics Technology Institute (KETI), Korea

Korea Information Security Agency (KISA), Korea

BK21 Information Security in Ubiquitous Environment, Korea

Mobile Network Security Technology Research Center (MSRC), Korea

LG-CNS, Korea

LOTTE Data Communication Company, Korea

SNU-BK21 Mathematical Sciences Division, Korea

Sungkyunkwan University Authentication Technology Research Center

(SKKU ARTC), Korea

# Table of Contents

## Public Key Encryption

Simple CCA-Secure Public Key Encryption from Any Non-Malleable Identity-Based Encryption . . . . .	1
<i>Takahiro Matsuda, Goichiro Hanaoka, Kanta Matsuura, and Hideki Imai</i>	
Distributed Attribute-Based Encryption . . . . .	20
<i>Sascha Müller, Stefan Katzenbeisser, and Claudia Eckert</i>	
Improved Partial Key Exposure Attacks on RSA by Guessing a Few Bits of One of the Prime Factors . . . . .	37
<i>Santanu Sarkar and Subhamoy Maitra</i>	
Simple Algorithms for Computing a Sequence of 2-Isogenies . . . . .	52
<i>Reo Yoshida and Katsuyuki Takashima</i>	

## Key Management and Secret Sharing

Survival in the Wild: Robust Group Key Agreement in Wide-Area Networks . . . . .	66
<i>Jihye Kim and Gene Tsudik</i>	
Visual Secret Sharing Schemes with Cyclic Access Structure for Many Images . . . . .	84
<i>Miyuki Uno and Mikio Kano</i>	

## Privacy and Digital Rights

The Swiss-Knife RFID Distance Bounding Protocol . . . . .	98
<i>Chong Hee Kim, Gildas Avoine, François Koeune, François-Xavier Standaert, and Olivier Pereira</i>	
Protecting Location Privacy through a Graph-Based Location Representation and a Robust Obfuscation Technique . . . . .	116
<i>Jafar Haadi Jafarian, Ali Noorollahi Ravari, Morteza Amini, and Rasool Jalili</i>	
Anonymous Fingerprinting for Predelivery of Contents . . . . .	134
<i>Kazuhiro Haramura, Maki Yoshida, and Toru Fujiwara</i>	
Instruction Set Limitation in Support of Software Diversity . . . . .	152
<i>Bjorn De Sutter, Bertrand Anckaert, Jens Geiregat, Dominique Chagnet, and Koen De Bosschere</i>	

## Digital Signature and Voting

Non-interactive Identity-Based DNF Signature Scheme and Its Extensions . . . . .	166
<i>Kwangsu Lee, Jung Yeon Hwang, and Dong Hoon Lee</i>	
How to Balance Privacy with Authenticity . . . . .	184
<i>Pairat Thorncharoensri, Willy Susilo, and Yi Mu</i>	
Efficient Vote Validity Check in Homomorphic Electronic Voting . . . . .	202
<i>Kun Peng and Feng Bao</i>	

## Side Channel Attack

Secure Hardware Implementation of Non-linear Functions in the Presence of Glitches . . . . .	218
<i>Svetla Nikova, Vincent Rijmen, and Martin Schl�affer</i>	
Novel PUF-Based Error Detection Methods in Finite State Machines . . .	235
<i>Ghaith Hammouri, Kahraman Akdemir, and Berk Sunar</i>	
Partition vs. Comparison Side-Channel Distinguishers: An Empirical Evaluation of Statistical Tests for Univariate Side-Channel Attacks against Two Unprotected CMOS Devices . . . . .	253
<i>Fran�ois-Xavier Standaert, Benedikt Gierlichs, and Ingrid Verbauwhede</i>	

## Hash and MAC

A Single-Key Domain Extender for Privacy-Preserving MACs and PRFs . . . . .	268
<i>Kan Yasuda</i>	
Extended Models for Message Authentication . . . . .	286
<i>Liting Zhang, Wenling Wu, and Peng Wang</i>	
A Preimage Attack for 52-Step HAS-160 . . . . .	302
<i>Yu Sasaki and Kazumaro Aoki</i>	

## Primitives and Foundations

Essentially Optimal Universally Composable Oblivious Transfer . . . . .	318
<i>Ivan Damg�ard, Jesper Buus Nielsen, and Claudio Orlandi</i>	
Generalized Universal Circuits for Secure Evaluation of Private Functions with Application to Data Classification . . . . .	336
<i>Ahmad-Reza Sadeghi and Thomas Schneider</i>	

Proving a Shuffle Using Representations of the Symmetric Group . . . . .	354
<i>Soojin Cho and Manpyo Hong</i>	
On Formal Verification of Arithmetic-Based Cryptographic Primitives . . . . .	368
<i>David Nowak</i>	
<b>Block and Stream</b>	
A New Technique for Multidimensional Linear Cryptanalysis with Applications on Reduced Round Serpent . . . . .	383
<i>Joo Yeon Cho, Mia Hermelin, and Kaisa Nyberg</i>	
Almost Fully Optimized Infinite Classes of Boolean Functions Resistant to (Fast) Algebraic Cryptanalysis . . . . .	399
<i>Enes Pasalic</i>	
Higher Order Differential Attacks on Reduced-Round MISTY1 . . . . .	415
<i>Yukiyasu Tsunoo, Teruo Saito, Maki Shigeri, and Takeshi Kawabata</i>	
<b>Author Index</b> . . . . .	433