

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

TU Dortmund University, Germany

Madhu Sudan

Microsoft Research, Cambridge, MA, USA

Demetri Terzopoulos

University of California, Los Angeles, CA, USA

Doug Tygar

University of California, Berkeley, CA, USA

Gerhard Weikum

Max Planck Institute for Informatics, Saarbruecken, Germany

Kyung-Hyune Rhee DaeHun Nyang (Eds.)

Information Security and Cryptology - ICISC 2010

13th International Conference
Seoul, Korea, December 1-3, 2010
Revised Selected Papers

Volume Editors

Kyung-Hyune Rhee
Pukyong National University
Department of IT Convergence Application Engineering
599-1 Daeyeon 3-Dong Namgu, Busan 608-737, Republic of Korea
E-mail: khrhee@pknu.ac.kr

DaeHun Nyang
INHA University
Department of Computer Science and Information Technology
253 Yonghyun-dong, Nam-gu, Incheon 402-751, Republic of Korea
E-mail: nyang@inha.ac.kr

ISSN 0302-9743
ISBN 978-3-642-24208-3
DOI 10.1007/978-3-642-24209-0
Springer Heidelberg Dordrecht London New York

e-ISSN 1611-3349
e-ISBN 978-3-642-24209-0

Library of Congress Control Number: 2011936884

CR Subject Classification (1998): E.3, K.6.5, C.2, D.4.6, G.2.1, E.4

LNCS Sublibrary: SL 4 – Security and Cryptology

© Springer-Verlag Berlin Heidelberg 2011

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.

The use of general descriptive names, registered names, trademarks, etc. in this publication does not imply, even in the absence of a specific statement, that such names are exempt from the relevant protective laws and regulations and therefore free for general use.

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

Printed on acid-free paper

Springer is part of Springer Science+Business Media (www.springer.com)

Preface

ICISC 2010, the 13th International Conference on Information Security and Cryptology, was held in Seoul, Korea, during December 1–3, 2010. 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 intended to be a place where research information can be exchanged.

The conference received 99 submissions from 27 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 64 prominent experts 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 PC finally selected 28 papers from 16 countries. The acceptance rate was 28.2%. The authors of selected papers had a few weeks to prepare for their final versions based on the comments received from the 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 delivered by Tatsuaki Okamoto from NTT Information Sharing Platform Laboratories. The invited speakers were Sakir Sezer from ECIT SoC Research Division and Giuseppe Ateniese from The Johns Hopkins University.

There are many people who contributed to the success of ICISC 2010. We would like to thank all the authors who submitted papers to this conference. We are deeply grateful to all 64 members of the PC, especially to those who shepherded conditionally accepted papers. 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. We would also like to thank the iChair developers for allowing us to use their 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 and all organizing members who nicely managed the conference.

December 2010

Kyung-Hyune Rhee
DaeHun Nyang

Organization

ICISC 2010, The 13th Annual International Conference on Information Security and Cryptology, was held during December 1–3, 2010, at Chung-Ang University, Seoul, Korea, and organized by Korea Institute of Information Security and Cryptology (KIISC) (<http://www.kiisc.or.kr>) in cooperation with the Ministry of Public Administration and Security (MOPAS) (<http://www.mopas.go.kr>)

General Chair

Jong In Lim
KIISC, Korea

Program Co-chairs

Kyung-Hyune Rhee
DaeHun Nyang
Pukyong National University, Korea
INHA university, Korea

Program Committee

Joonsang Baek	Institute for Infocomm Research, Singapore
Alex Biryukov	University of Luxembourg, Luxembourg
Seongtaek Chee	Attached Institute of ETRI, Korea
Jung Hee Cheon	Seoul National University, Korea
Yongwha Chung	Korea University, Korea
Paolo Milani Comparetti	Vienna University of Technology, Austria
Frédéric Cuppens	Telecom Bretagne, France
Paolo D'Arco	University of Salerno, Italy
Bart De Decker	Katholieke Universiteit Leuven, Belgium
David Galindo	University of Luxembourg, Luxembourg
Philippe Golle	Palo Alto Research Center, USA
Vipul Goyal	UCLA, USA
Louis Granboulan	EADS Innovation Works, France
Matthew Green	Independent Security Evaluators, USA
JaeCheol Ha	Hoseo University, Korea
Dong-Guk Han	Kookmin University, Korea
Martin Hell	Lunds Universitet, Sweden
Deukjo Hong	Attached Institute of ETRI, Korea
Jin Hong	Seoul National University, Korea
Seokhie Hong	Korea University, Korea
Jung Yeon Hwang	ETRI, Korea
David Jao	University of Waterloo, Canada

VIII Organization

Ju-Sung Kang	Kookmin University, Korea
Ho-Won Kim	Pusan University, Korea
Jihye Kim	Seoul National University, Korea
Seungjoo Kim	Sungkyunkwan University, Korea
Taekyoung Kwon	Sejong University, Korea
Xuejia Lai	Shanghai Jiao Tong University, China
Byoungcheon Lee	Joongbu University, Korea
Im-Yeong Lee	Soonchunyang University, Korea
Mun-Kyu Lee	Inha University, Korea
Pil Joong Lee	Pohang University of Science and Technology, Korea
Mark Manulis	TU Darmstadt, Germany
Keith Martin	Royal Holloway, University of London, UK
Sjouke Mauw	University of Luxembourg, Luxembourg
Atsuko Miyaji	JAIST, Japan
Jose A. Montenegro	University of Malaga, Spain
David Naccache	ENS, France
Heekuck Oh	Hanyang University, Korea
Rolf Oppliger	eSECURITY Technologies, Switzerland
Raphael C.-W. Phan	Loughborough University, UK
Bart Preneel	K.U. Leuven, Belgium
Vincent Rijmen	K.U.Leuven and TU Graz, Belgium and Austria
Bimal Roy	Indian Statistical Institute, India
Ahmad-Reza Sadeghi	Ruhr University Bochum, Germany
Kouichi Sakurai	Kyushu University, Japan
Palash Sarkar	Indian Statistical Institute, India
Kyung-Ah Shim	NIMS, Korea
Sang-Uk Shin	Pukyong University, Korea
Hong-Yeop Song	Yonsei 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
Jorge Villar	Universitat Politecnica de Catalunya, Spain
Sung-Ming Yen	National Central University, Taiwan
Jeong Hyun Yi	Soongsil University, Korea
Kangbin Yim	Soonchunyang University, Korea
Myungkeun Yoon	Kookmin University, Korea
Dae Hyun Yum	Pohang University of Science and Technology, Korea
Fangguo Zhang	Sun Yat-sen University, China
Jianying Zhou	I2R, Singapore

Organizing Committee Chair

Sehyun Park

Chung-Ang University, Seoul, Korea

Organizing Committee Vice-Chair

Eul Gyu Im

Hanyang University, Seoul, Korea

Organizing Committee

Jong-Soo Jang

ETRI, Korea

Dong-Kyue Kim

Hanyang University, Korea

Daesung Kwon

Attached Institute of ETRI, Korea

Im-Yeong Lee

Soonchunhyang University, Korea

Mun-Kyu Lee

Inha University, Korea

Yongsu Park

Hanyang University, Korea

Jungtaek Seo

Attached Institute of ETRI, Korea

Kyung-Ah Shim

NIMS, Korea

Yoo-jae Won

KISA, Korea

Jeong Hyun Yi

Soongsil University, Korea

External Reviewers

Anna Lisa Ferrara

Hyung Tae Lee

Antonio Muñoz

Hyun-Min Kim

Benedikt Gierlichs

Isaac Agudo

Bin Zhang

Ivica Nikolic

Bo Zhu

Jae Ahn Hyun

Bonwook Koo

Jae Hong Seo

Cheol-Min Park

Jae Woo Seo

Chunhua Su

Jangseung Kim

Claudio Soriente

Jeonil Kang

Daeseon Choi

Jheng-Hong Tu

Daesung Kwon

Ji Young Chun

Eun Sung Lee

Jihye Kim

Gunil Ma

Joaquin Garcia-Alfaro

Hakan Seyalioglu

Johann Großschädl

Hans Loehr

Joseph K. Liu

Hee-Seok Kim

Jun Pang

HongTae Kim

Jung Youl Park

Hsi-Chung Lin

Kai Yuen Cheong

Hugo Jonker

Kazuhiko Minematsu

Hyeong-Chan Lee

Kazumasa Omote

Hyun-Dong So

Kenneth Matheis

Lingling Xu	Sungwook Eom
Luca Davi	Sung-Wook Lee
Maki Shigeri	Taechan Kim
Martin Ågren	Takashi Nishide
Ming Duan	Takeshi Kawabata
Mingwu Zhang	Taku Hayashi
Minkyu Kim	Tamer AbuHmed
Moonsung Lee	Teruo Saito
MyungKeun Yoon	Thomas Baigneres
Myungsun Kim	Thomas Schneider
Nicky Mouha	Ton van Deursen
Özgür Dagdelen	Vincent Naessens
Paul Stankovski	Wei-Chih Lien
Pedro Peris-Lopez	Xingwen Zhao
Pieter Verhaeghe	Xinyi Huang
Ping Wang	Yanjiang Yang
Qiping Lin	Yasufumi Hashimoto
Ralf-Philipp Weinmann	Yeonkyu Kim
Rishiraj Bhattacharyya	Ying Qiu
Ruei-Hau Hsu	Young-In Cho
Ryoji Ohta	YoungJae Maeng
Sangrae Cho	Young-Ran Lee
Sasa Radomirovic	YoungSeob Cho
Sebastian Faust	Younho Lee
Seog Chung Seo	Youn-Taek Young
Somindu C. Ramanna	Yu Sasaki
Sanjay Bhattacharjee	Kenji Ohkuma
Subhabrata Samajder	Zayabaatar
Sung-Kyung Kim	Zheng Gong

Sponsoring Institutions

National Security Research Institute (NSRI)
Electronics and Telecommunications Research Institute (ETRI)
Korea Internet & Security Agency (KISA)
Korean Federation of Science and Technology Societies (KOFST)
Chung-Ang University Home Network Research Center (CAU HNRC)
Chungnam National University Internet Intrusion Response Technology
Research Center (CNU IIRTRC)
Korea University Center for Information Security Technologies (KU CIST)

Table of Contents

Cryptanalysis

Analysis of Nonparametric Estimation Methods for Mutual Information Analysis	1
<i>Alexandre Venelli</i>	
Bias Analysis of a Certain Problem with Applications to E0 and Shannon Cipher	16
<i>Yi Lu and Yvo Desmedt</i>	
Known and Chosen Key Differential Distinguishers for Block Ciphers ...	29
<i>Ivica Nikolić, Josef Pieprzyk, Przemysław Sokołowski, and Ron Steinfeld</i>	
Related-Key Attack on the Full HIGHT	49
<i>Bonwook Koo, Deukjo Hong, and Daesung Kwon</i>	
Preimage Attacks against PKC98-Hash and HAS-V	68
<i>Yu Sasaki, Florian Mendel, and Kazumaro Aoki</i>	
Passive Cryptanalysis of the UnConditionally Secure Authentication Protocol for RFID Systems	92
<i>Mohammad Reza Sohizadeh Abyaneh</i>	
Cryptanalysis of RSA with Small Prime Combination	104
<i>Xianmeng Meng</i>	

Cryptographic Algorithms

The Twin Bilinear Diffie-Hellman Inversion Problem and Applications	113
<i>Yu Chen and Liqun Chen</i>	
Group Signatures Are Suitable for Constrained Devices	133
<i>Sébastien Canard, Iwen Coisel, Giacomo De Meulenaer, and Olivier Pereira</i>	
A Lightweight 256-bit Hash Function for Hardware and Low-End Devices: Lesamnta-LW	151
<i>Shoichi Hirose, Kota Ideguchi, Hidenori Kuwakado, Toru Owada, Bart Preneel, and Hirotaka Yoshida</i>	

Implementation

Efficient Pairing Computation on Elliptic Curves in Hessian Form	169
<i>Haihua Gu, Dawu Gu, and WenLu Xie</i>	
FPGA Implementation of an Improved Attack against the DECT Standard Cipher	177
<i>Michael Weiner, Erik Tews, Benedikt Heinz, and Johann Heyszl</i>	
Chameleon: A Versatile Emulator for Contactless Smartcards	189
<i>Timo Kasper, Ingo von Maurich, David Oswald, and Christof Paar</i>	

Network and Mobile Security

Revisiting Address Space Randomization	207
<i>Zhi Wang, Renquan Cheng, and Debin Gao</i>	
Evaluation of a Spyware Detection System Using Thin Client Computing	222
<i>Vasilis Pappas, Brian M. Bowen, and Angelos D. Keromytis</i>	
A Comparative Usability Evaluation of Traditional Password Managers	233
<i>Ambarish Karole, Nitesh Saxena, and Nicolas Christin</i>	
An Adversarial Evaluation of Network Signaling and Control Mechanisms	252
<i>Kangkook Jee, Stelios Sidiroglou-Douskos, Angelos Stavrou, and Angelos D. Keromytis</i>	
Secure Personalized Recommendation System for Mobile User	266
<i>Soe Yu Maw</i>	

Symmetric Key Cryptography

Protecting White-Box AES with Dual Ciphers	278
<i>Mohamed Karroumi</i>	
\mathcal{E} -MACs: Towards More Secure and More Efficient Constructions of Secure Channels	292
<i>Basel Alomair and Radha Poovendran</i>	
On Equivalence Classes of Boolean Functions	311
<i>Qichun Wang and Thomas Johansson</i>	

Cryptographic Protocols

Public Discussion Must Be Back and Forth in Secure Message Transmission	325
<i>Takeshi Koshihara and Shinya Sawada</i>	
Scalar Product-Based Distributed Oblivious Transfer	338
<i>Christian L.F. Corniaux and Hossein Ghodosi</i>	
Unconditionally Secure Rational Secret Sharing in Standard Communication Networks	355
<i>Zhifang Zhang and Mulan Liu</i>	
Oblivious Transfer with Complex Attribute-Based Access Control	370
<i>Lingling Xu and Fangguo Zhang</i>	

Side Channel Attack

Fault Attacks on the Montgomery Powering Ladder	396
<i>Jörn-Marc Schmidt and Marcel Medwed</i>	
First Principal Components Analysis: A New Side Channel Distinguisher	407
<i>Youssef Souissi, Maxime Nassar, Sylvain Guilley, Jean-Luc Danger, and Florent Flament</i>	
Fault Analysis on Stream Cipher MUGI	420
<i>Junko Takahashi, Toshinori Fukunaga, and Kazuo Sakiyama</i>	
Author Index	435