Lecture Notes in Computer Science 7259

Commenced Publication in 1973
Founding and Former Series Editors:
Gerhard Goos, Juris Hartmanis, and Jan van Leeuwen

Howon Kim (Ed.)

Information Security and Cryptology – ICISC 2011

14th International Conference
Seoul, Korea, November 30 – December 2, 2011
Revised Selected Papers

Springer

Volume Editor

Howon Kim
Pusan National University
(A06) 6503 School of Computer Science
and Engineering
San-30, JangJeon-Dong, GeumJeong-Gu
Busan, 609-735, South Korea
E-mail: howonkim@pusan.ac.kr

ISSN 0302-9743 e-ISSN 1611-3349
ISBN 978-3-642-31911-2 e-ISBN 978-3-642-31912-9
DOI 10.1007/978-3-642-31912-9
Springer Heidelberg Dordrecht London New York

Library of Congress Control Number: 2012941979

CR Subject Classification (1998): E.3, K.6.5, C.2, D.4.6, G.2.1, E.4, J.1

LNCS Sublibrary: SL 4 – Security and Cryptology

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 2011, the 14th International Conference on Information Security and Cryptology, was held in Seoul, Korea, during November 30 – December 2, 2011. It was organized by the Korea Institute of Information Security and Cryptology (KIISC).

The aim of this conference was to create a forum for the dissemination of the latest results in research, development, and applications in the field of information security, and cryptology. The conference received 126 submissions from 29 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 52 prominent experts via the Springer OCS. First, each paper was blind reviewed by at least three PC members. Second, for resolving conflicts on each reviewer's decision, individual review reports were revealed to PC members, and detailed interactive discussion on each paper followed. Through this process, the PC finally selected 32 papers from 10 countries.

The acceptance rate was 25.4%. For the LNCS proceedings, the authors of selected papers had a few weeks to prepare for their final versions based on the comments received from the reviewers. The conference featured two invited talks delivered by Thomas Peyrin from Nanyang Technological University and Atsuko Miyaji from Japan Advanced Institute of Science and Technology.

Many people have contributed to the organization of ICISC 2011 and the preparation of this volume. We would like to thank all the authors who submitted papers to this conference. We are deeply grateful to all 52 members of the PC. 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.

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 Committee members who nicely managed the conference.

November 2011 Howon Kim

ICISC 2011 Organization

General Chair

Heung-Youl Youm	Soon-Chun-Hyang University, Korea

Organizing Chair

Sang-Choon Kim	Kangwon National University, Korea

Program Chair

Howon Kim	Pusan National University, Korea

Steering Committee

Man Young Rhee	Kyunghee University, Korea
Pil Joong Lee	Pohang University, Korea
Dongho Won	Sungkyunkwan University, Korea
Ju Seok Song	Yonsei University, Korea
Koji Nakao	National Institute of Information and Communications Technology, Japan

Program Committee

Joonsang Baek	KUSTAR, UAE
Alex Biryukov	University of Luxembourg, Luxembourg
Jung Hee Cheon	Seoul National University, Korea
Dooho Choi	ETRI, Korea
Yongwha Chung	Korea University, Korea
Frëdëric Cuppens	Telecom Bretagne, France
Paolo D'Arco	University of Salerno, Italy
Bart De Decker	K.U. Leuven, Belgium
David Galindo	University of Luxembourg, Luxembourg
Louis Granboulan	EADS Innovation Works, France
Matthew Green	Johns Hopkins University, USA
Johann Großschädl	University of Luxembourg, Luxembourg
JaeCheol Ha	Hoseo University, Korea
Dong-Guk Han	Kookmin University, Korea
Martin Hell	Lund University, Sweden
Seokhie Hong	Korea University, Korea
Jin Hong	Seoul National University, Korea

Jung Yeon Hwang	ETRI, Korea
David Jao	University of Waterloo, Canada
Ju-Sung Kang	Kookmin University, Korea
Ji Hye Kim	Seoul National University, Korea
Seungjoo Kim	Korea University, Korea
Taekyoung Kwon	Sejong University, Korea
Im-Yeong Lee	Soonchunyang University, Korea
Mun-Kyu Lee	Inha University, Korea
Pil Joong Lee	POSTECH, Korea
Mark Manulis	TU Darmstadt and CASED, Germany
Keith Martin	University of London, UK
Sjouke Mauw	University of Luxembourg, Luxembourg
Atsuko Miyaji	JAIST, Japan
Jose A. Montenegro	Universidad de Malaga, Spain
Kirill Morozov	Kyushu University, Japan
David Naccache	ENS DI, France
Rolf Oppliger	eSECURITY Technologies, Switzerland
Omkant Pandey	Microsoft, USA and India
Raphael C.-W. Phan	Loughborough University, UK
Bimal Roy	Indian Statistical Institute, India
Ahmad-Reza Sadeghi	Technische Universität Darmstadt, Germany
Kouichi Sakurai	Kyushu University, Japan
Palash Sarkar	Indian Statistical Institute, India
Kyung-Ah Shim	NIMS, Korea
Sang-Uk Shin	Pukyong National University, Korea
Rainer Steinwandt	Florida Atlantic University, USA
Willy Susilo	University of Wollongong, Australia
Tsuyoshi Takagi	Kyushu University, Japan
Yukiyasu Tsunoo	NEC Corp., Japan
Jorge Villar	Universitat Politecnica de Catalunya, Spain
Rijmen Vincent	Katholieke University Leuven
Jeong Hyun Yi	Soongsil University, Korea
Dae Hyun Yum	POSTECH, Korea
Jianying Zhou	Institute for Infocomm Research, Singapore
Jehong Park	ETRI, Korea

Sponsored by

National Security Research Institute (NSRI)
Electronics and Telecommunications Research Institute (ETRI)
Korea Internet & Security Agency (KISA)
Ministry of Public Administration and Security (MOPAS)

Table of Contents

Digital Signature

Side Channel Analysis II

Cryptanalysis

Efficient Implementation

Hash Function II

Cryptographic Application

Cryptographic Protocol