

*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*

Taekyoung Kwon Mun-Kyu Lee  
Daesung Kwon (Eds.)

# Information Security and Cryptology – ICISC 2012

15th International Conference  
Seoul, Korea, November 28-30, 2012  
Revised Selected Papers



Springer

Volume Editors

Taekyoung Kwon  
Sejong University  
Department of Computer Engineering  
Seoul 143-747, Korea  
E-mail: tkwon@sejong.edu

Mun-Kyu Lee  
Inha University  
School of Computer and Information Engineering  
Incheon 402-751, Korea  
E-mail: mkleee@inha.ac.kr

Daesung Kwon  
National Security Research Institute  
Daejeon 306-600, Korea  
E-mail: ds\_kwon@ensec.re.kr

ISSN 0302-9743  
ISBN 978-3-642-37681-8  
DOI 10.1007/978-3-642-37682-5  
Springer Heidelberg Dordrecht London New York

e-ISSN 1611-3349  
e-ISBN 978-3-642-37682-5

Library of Congress Control Number: 2013935780

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

© Springer-Verlag Berlin Heidelberg 2013

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 2012, the 15th International Conference on Information Security and Cryptology, was held in Seoul, Korea, during November 28–30, 2012. This year the conference was hosted by the KIISC (Korea Institute of Information Security and Cryptology) jointly with the NSRI (National Security Research Institute), in cooperation with the Ministry of Public Administration and Security (MOPAS).

The aim of this conference is to provide an international forum for the latest results of research, development, and applications in the field of information security and cryptology. This year we received 120 submissions from more than 20 countries and were able to accept 32 papers from 13 countries, with the acceptance rate of 26.7%. The review and selection processes were carried out by the Program Committee (PC) members, 88 prominent experts world-wide, via Springer’s OCS system. First, each paper was blind reviewed by at least three PC members. Second, to resolve conflicts in the reviewer’s decisions, the individual review reports were open to all PC members, and detailed interactive discussions on each paper ensued. For the LNCS post-proceedings, the authors of selected papers had a few weeks to prepare their final versions based on the comments received from the reviewers. We also recommended that authors should revise their papers based on the comments and recommendations they might have received from attendees upon their presentations at the conference.

The conference featured three invited talks: “Machine Learning on Encrypted Data” delivered by Kristin Lauter, Microsoft Research; “Another Look at Affine-Padding RSA Signatures” by David Naccache, Ecole Normale Supérieure; and “New Meet-in-the-Middle Attacks in Symmetric Cryptanalysis” by Christian Rechberger, Technical University of Denmark. We thank the invited speakers for their kind acceptance and nice presentations.

We would like to thank all the authors who submitted their papers to ICISC 2012 and all 88 PC members. It was a truly nice experience to work with such talented and hard-working researchers. We also appreciate the external reviewers for assisting the PC members in their particular areas of expertise. Finally, we would like to thank all attendees for their active participation and the Organizing Committee Members, who nicely managed this conference. We look forward to next year’s ICISC.

January 2013

Taekyoung Kwon  
Mun-Kyu Lee  
Daesung Kwon

# ICISC 2012

The 15th Annual International Conference  
on Information Security

November 28–30, 2012  
Konkuk University, Seoul, Korea

*Hosted by*

Korea Institute of Information Security and Cryptology (KIISC)  
National Security Research Institute (NSRI)

*Supported by*

Ministry of Public Administration and Security (MOPAS)  
Electronics and Telecommunications Research Institute (ETRI)  
Korea Internet & Security Agency (KISA)  
The Korean Federation of Science and Technology Societies (KOFST)

## General Chairs

Chang-Seop Park  
Seokyoul Kang

KIISC and Dankook University, Korea  
NSRI, Korea

## Program Co-chairs

Taekyoung Kwon  
Mun-Kyu Lee  
Daesung Kwon

Sejong University, Korea  
Inha University, Korea  
NSRI, Korea

## Program Committee

Frederik Armknecht  
Joonsang Baek  
Alex Biryukov  
Zhenfu Cao  
Aldar C-F. Chan  
Ku-Young Chang  
Kefei Chen  
Jung Hee Cheon  
Yongwha Chung  
Nora Cuppens-Bouahia

University of Mannheim, Germany  
KUSTAR, UAE  
University of Luxembourg, Luxembourg  
Shanghai Jiao Tong University, China  
Institute for Infocomm Research, Singapore  
ETRI, Korea  
Shanghai Jiaotong University, China  
Seoul National University, Korea  
Korea University, Korea  
TELECOM Bretagne, France

Paolo D'Arco	University of Salerno, Italy
Bart De Decker	IBBT-DistriNet, KU Leuven, Belgium
Rafael Dowsley	University of California, San Diego, USA
Shaojing Fu	National University of Defense Technology, China
David Galindo	University of Luxembourg, Luxembourg
Dieter Gollmann	Security in Distributed Applications
Louis Granboulan	EADS Innovation Works, France
Johann Groszschaeed	University of Luxembourg, Luxembourg
JaeCheol Ha	Hoseo University, Korea
Dong-Guk Han	Kookmin University, Korea
Martin Hell	Lund University, Sweden
Swee-Huay Heng	Multimedia University, Malaysia
Deukjo Hong	NSRI, Korea
Dowon Hong	Kongju National University, Korea
Jin Hong	Seoul National University, Korea
Seokhie Hong	Korea University, Korea
Jiankun Hu	UNSW, Australia
Jung Yeon Hwang	ETRI, Korea
Eul Gyu Im	Hanyang University, Korea
David Jao	University of Waterloo, Canada
Hiroaki Kikuchi	Tokai University, Japan
Ji Hye Kim	Kookmin University, Korea
Howon Kim	Pusan National University, Korea
Huy Kang Kim	Korea University, Korea
Shinsaku Kiyomoto	KDDI R&D Laboratories Inc., Japan
Hyang-Sook Lee	Ewha Womans University, Korea
JongHyup Lee	Korea National University of Transportation, Korea
Jooyoung Lee	Sejong University, Korea
Pil Joong Lee	POSTECH, Korea
Su Mi Lee	Financial Security Agency, Korea
Dongdai Lin	Institute of Software, ISCAS, China
Mark Manulis	University of Surrey, UK
Sjouke Mauw	University of Luxembourg, Luxembourg
Atsuko Miyaji	JAIST, Japan
Yutaka Miyake	KDDI R&D Laboratories Inc., Japan
Abedelaziz Mohaisen	Verisign labs, USA
Jose A. Montenegro	Universidad de Malaga, Spain
Fidel Nemenzo	University of the Philippines, Philippines
DaeHun Nyang	Inha University, Korea
Heekuck Oh	Hanyang University, Korea
Tae (Tom) Oh	Rochester Institute of Technology, USA
Rolf Oppliger	eSECURITY Technologies, Switzerland
Daniel Page	University of Bristol, UK

Susan Pancho-Festin	University of the Philippines, Philippines
Omkant Pandey	Microsoft Research India, India / University of Texas, Austin, USA
Raphael C.-W. Phan	Multimedia University, Malaysia
Christian Platzter	Automation Systems Group at the Technical University of Vienna, Austria
Carla Ráfols	Ruhr-Universität Bochum, Germany
C. Pandu Rangan	Indian Institute of Technology Madras, India
Christian Rechberger	DTU, Denmark
Vincent Rijmen	Katholieke Universiteit Leuven, Belgium
Bimal Roy	Indian Statistical Institute, India
Kouichi Sakurai	Kyushu University, Japan
Palash Sarkar	Indian Statistical Institute, India
Nitesh Saxena	University of Alabama, Birmingham, USA
Ji Sun Shin	Sejong University, Korea
Sang Uk Shin	Pukyong National University, Korea
Hong-Yeop Song	Yonsei University, Korea
Rainer Steinwandt	Florida Atlantic University, USA
Hung-Min Sun	National Tsing Hua University, Taiwan
Willy Susilo	University of Wollongong, Australia
Tsuyoshi Takagi	Kyushu University, Japan
Yukiyasu Tsunoo	NEC Corporation, Japan
Marion Videau	University of Lorraine / LORIA, France
Jorge Villar	Universitat Politècnica de Catalunya, Spain
Yongzhuang Wei	Guilin University of Electronic Technology, China
Wenling Wu	SKLOIS, Chinese Academy of Sciences, China
Toshihiro Yamauchi	Okayama University, Japan
Wei-Chuen Yau	Multimedia University, Malaysia
Ching-Hung Yeh	Far East University, Taiwan
Sung-Ming Yen	National Central University, Taiwan
Yongjin Yeom	Kookmin University, Korea
Jeong Hyun Yi	Soongsil University, Korea
Kazuki Yoneyama	NTT, Japan
Myungkeun Yoon	Kookmin University, Korea
Dae Hyun Yum	Myongji University, Korea
Aaram Yun	UNIST, Korea
Fanguo Zhang	Sun Yat-sen University, China

## Organizing Chair

Dong Il Seo ETRI, Korea

## Organizing Committee

Heuisu Ryu	Gyeongin National University of Education, Korea
Hokun Moon	KT, Korea
Howon Kim	Pusan National University, Korea
Jason Kim	Korea Internet & Security Agency, Korea
Keecheon Kim	Konkuk University, Korea
Soohyun Oh	Hoseo University, Korea
Tae-Hoon Kim	SYWORKS, Korea
Young-Ho Park	Sejong Cyber University, Korea



# Table of Contents

## Invited Papers

ML Confidential: Machine Learning on Encrypted Data . . . . .	1
<i>Thore Graepel, Kristin Lauter, and Michael Naehrig</i>	
Another Look at Affine-Padding RSA Signatures . . . . .	22
<i>Jean-Sébastien Coron, David Naccache, and Mehdi Tibouchi</i>	
On Brute-force-Like Cryptanalysis: New Meet-in-the-Middle Attacks in Symmetric Cryptanalysis . . . . .	33
<i>Christian Rechberger</i>	

## Attack and Defense

Balanced Indexing Method for Efficient Intrusion Detection Systems . . .	37
<i>BooJoong Kang, Hye Seon Kim, Ji Su Yang, and Eul Gyu Im</i>	
Quantitative Questions on Attack-Defense Trees . . . . .	49
<i>Barbara Kordy, Sjouke Mauw, and Patrick Schweitzer</i>	
DNS Tunneling for Network Penetration . . . . .	65
<i>Daan Raman, Bjorn De Sutter, Bart Coppens, Stijn Volckaert, Koen De Bosschere, Pieter Danhieux, and Erik Van Buggenhout</i>	
MeadDroid: Detecting Monetary Theft Attacks in Android by DVM Monitoring . . . . .	78
<i>Lingguang Lei, Yuewu Wang, Jiwu Jing, Zhongwen Zhang, and Xingjie Yu</i>	

## Software and Web Security

iBinHunt: Binary Hunting with Inter-procedural Control Flow . . . . .	92
<i>Jiang Ming, Meng Pan, and Debin Gao</i>	
Sometimes It's Better to Be STUCK! SAML Transportation Unit for Cryptographic Keys . . . . .	110
<i>Christopher Meyer, Florian Feldmann, and Jörg Schwenk</i>	

## Cryptanalysis I

Improved Impossible Differential Attacks on Large-Block Rijndael . . . . .	126
<i>Qingju Wang, Dawu Gu, Vincent Rijmen, Ya Liu, Jiazhe Chen, and Andrey Bogdanov</i>	

Cube Cryptanalysis of LBlock with Noisy Leakage . . . . .	141
<i>Zhenqi Li, Bin Zhang, Yuan Yao, and Dongdai Lin</i>	
Comprehensive Study of Integral Analysis on 22-Round LBlock . . . . .	156
<i>Yu Sasaki and Lei Wang</i>	
New Impossible Differential Attack on SAFER <sub>+</sub> and SAFER <sub>++</sub> . . . . .	170
<i>Jingyuan Zhao, Meiqin Wang, Jiazhe Chen, and Yuliang Zheng</i>	

## Cryptographic Protocol

An Information-Theoretically Secure Threshold Distributed Oblivious Transfer Protocol . . . . .	184
<i>Christian L.F. Corniaux and Hossein Ghodsi</i>	
Practically Efficient Multi-party Sorting Protocols from Comparison Sort Algorithms . . . . .	202
<i>Koki Hamada, Ryo Kikuchi, Dai Ikarashi, Koji Chida, and Katsumi Takahashi</i>	
Provably Secure Certificateless One-Way and Two-Party Authenticated Key Agreement Protocol . . . . .	217
<i>Lei Zhang</i>	

## Identity-Based Encryption

A CCA-Secure Identity-Based Conditional Proxy Re-Encryption without Random Oracles . . . . .	231
<i>Kaitai Liang, Zhen Liu, Xiao Tan, Duncan S. Wong, and Chunming Tang</i>	
Ciphertext Policy Multi-dimensional Range Encryption . . . . .	247
<i>Kohei Kasamatsu, Takahiro Matsuda, Goichiro Hanaoka, and Hideki Imai</i>	

## Efficient Implementation

Speeding Up Ate Pairing Computation in Affine Coordinates . . . . .	262
<i>Duc-Phong Le and Chik How Tan</i>	
An Improved Hardware Implementation of the Grain-128a Stream Cipher . . . . .	278
<i>Shohreh Sharif Mansouri and Elena Dubrova</i>	
Optimized GPU Implementation and Performance Analysis of HC Series of Stream Ciphers . . . . .	293
<i>Ayesha Khalid, Deblin Bagchi, Goutam Paul, and Anupam Chattopadhyay</i>	

## Cloud Computing Security

Trusted Launch of Virtual Machine Instances in Public IaaS Environments .....	309
<i>Nicolae Paladi, Christian Gehrman, Mudassar Aslam, and Fredric Morenius</i>	
Secure and Privacy-Aware Multiplexing of Hardware-Protected TPM Integrity Measurements among Virtual Machines .....	324
<i>Michael Velten and Frederic Stumpf</i>	

## Cryptanalysis II

Improved Key Recovery Attacks on Reduced-Round Salsa20 and ChaCha .....	337
<i>Zhenqing Shi, Bin Zhang, Dengguo Feng, and Wenling Wu</i>	
Multi-differential Cryptanalysis on Reduced DM-PRESENT-80: Collisions and Other Differential Properties .....	352
<i>Takuma Koyama, Yu Sasaki, and Noboru Kunihiro</i>	
Estimating the Probabilities of Low-Weight Differential and Linear Approximations on PRESENT-Like Ciphers .....	368
<i>Mohamed Ahmed Abdelraheem</i>	

## Side Channel Analysis

Security Evaluation of Cryptographic Modules against Profiling Attacks .....	383
<i>Yongdae Kim, Naofumi Homma, Takafumi Aoki, and Heebong Choi</i>	
Key-Dependent Weakness of AES-Based Ciphers under Clockwise Collision Distinguisher .....	395
<i>Toshiki Nakasone, Yang Li, Yu Sasaki, Mitsugu Iwamoto, Kazuo Ohta, and Kazuo Sakiyama</i>	

## Digital Signature

Efficient Group Signatures in the Standard Model .....	410
<i>Laila El Aimagi and Olivier Sanders</i>	
Batch Verification Suitable for Efficiently Verifying a Limited Number of Signatures .....	425
<i>Keisuke Hakuta, Yosuke Katoh, Hisayoshi Sato, and Tsuyoshi Takagi</i>	
Linear Recurring Sequences for the UOV Key Generation Revisited ...	441
<i>Albrecht Petzoldt and Stanislav Bulygin</i>	

Galindo-Garcia Identity-Based Signature Revisited . . . . . 456  
*Sanjit Chatterjee, Chethan Kamath, and Vikas Kumar*

**Privacy Enhancement**

Private Over-Threshold Aggregation Protocols . . . . . 472  
*Myungsun Kim, Abdelaziz Mohaisen, Jung Hee Cheon, and  
Yongdae Kim*

Retracted: An Enhanced Anonymous Authentication and Key Exchange  
Scheme Using Smartcard . . . . . 487  
*Kyung-kug Kim and Myung-Hwan Kim*

Efficient Proofs for CNF Formulas on Attributes in Pairing-Based  
Anonymous Credential System . . . . . 495  
*Nasima Begum, Toru Nakanishi, and Nobuo Funabiki*

**Erratum**

An Enhanced Anonymous Authentication and Key Exchange Scheme  
Using Smartcard . . . . . E1  
*Kyung-kug Kim and Myung-Hwan Kim*

**Author Index** . . . . . 511