

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

Howon Kim (Ed.)

Information Security and Cryptology – ICISC 2011

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

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

© Springer-Verlag Berlin Heidelberg 2012

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 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
Doocho Choi	ETRI, Korea
Yongwha Chung	Korea University, Korea
Frédéric 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

Hash Function I

Improved Integral Analysis on Tweaked Lesamnta	1
<i>Yu Sasaki and Kazumaro Aoki</i>	
Analysis of Trivium Using Compressed Right Hand Side Equations	18
<i>Thorsten Ernst Schilling and Håvard Raddum</i>	
Cryptanalysis of Round-Reduced HAS-160	33
<i>Florian Mendel, Tomislav Nad, and Martin Schl�affer</i>	

Side Channel Analysis I

An Efficient Method for Eliminating Random Delays in Power Traces of Embedded Software	48
<i>Daehyun Strobel and Christof Paar</i>	
An Efficient Leakage Characterization Method for Profiled Power Analysis Attacks	61
<i>Hailong Zhang, Yongbin Zhou, and Dengguo Feng</i>	
Correcting Errors in Private Keys Obtained from Cold Boot Attacks . . .	74
<i>Hyung Tae Lee, HongTae Kim, Yoo-Jin Baek, and Jung Hee Cheon</i>	

Public Key Cryptography

Strong Security Notions for Timed-Release Public-Key Encryption Revisited	88
<i>Ryo Kikuchi, Atsushi Fujioka, Yoshiaki Okamoto, and Taiichi Saito</i>	
Fully Secure Unidirectional Identity-Based Proxy Re-encryption	109
<i>Song Luo, Qingni Shen, and Zhong Chen</i>	

Network and Mobile Security

Detecting Parasite P2P Botnet in <i>eMule</i> -like Networks through Quasi-periodicity Recognition	127
<i>Yong Qiao, Yuexiang Yang, Jie He, Bo Liu, and Yingzhi Zeng</i>	
AutoDunt: Dynamic Latent Dependence Analysis for Detection of Zero Day Vulnerability	140
<i>Kai Chen, Yifeng Lian, and Yingjun Zhang</i>	

Digital Signature

Weaknesses in Current RSA Signature Schemes	155
<i>Juliane Krämer, Dmitry Nedospasov, and Jean-Pierre Seifert</i>	
Back Propagation Neural Network Based Leakage Characterization for Practical Security Analysis of Cryptographic Implementations	169
<i>Shuguo Yang, Yongbin Zhou, Jiye Liu, and Danyang Chen</i>	

Side Channel Analysis II

A Revocable Group Signature Scheme with the Property of Hiding the Number of Revoked Users	186
<i>Keita Emura, Atsuko Miyaji, and Kazumasa Omote</i>	
Generic Constructions for Verifiable Signcryption	204
<i>Laila El Aimagi</i>	
Non-delegatable Strong Designated Verifier Signature on Elliptic Curves	219
<i>Haibo Tian, Xiaofeng Chen, Zhengtao Jiang, and Yusong Du</i>	

Cryptanalysis

An Improved Known Plaintext Attack on PKZIP Encryption Algorithm	235
<i>Kyung Chul Jeong, Dong Hoon Lee, and Daewan Han</i>	
Synthetic Linear Analysis: Improved Attacks on CubeHash and Rabbit	248
<i>Yi Lu, Serge Vaudenay, Willi Meier, Liping Ding, and Jianchun Jiang</i>	
On the Resistance of Boolean Functions against Fast Algebraic Attacks	261
<i>Yusong Du, Fangguo Zhang, and Meicheng Liu</i>	
CCA Secure IB-KEM from the Computational Bilinear Diffie-Hellman Assumption in the Standard Model	275
<i>Yu Chen, Liqun Chen, and Zongyang Zhang</i>	

Efficient Implementation

Design, Implementation, and Evaluation of a Vehicular Hardware Security Module	302
<i>Marko Wolf and Timo Gendrullis</i>	

Efficient Modular Exponentiation-Based Puzzles for Denial-of-Service Protection	319
<i>Jothi Rangasamy, Douglas Stebila, Lakshmi Kuppusamy, Colin Boyd, and Juan Gonzalez Nieto</i>	

Implementing Information-Theoretically Secure Oblivious Transfer from Packet Reordering	332
<i>Paolo Palmieri and Olivier Pereira</i>	

Hash Function II

Compression Functions Using a Dedicated Blockcipher for Lightweight Hashing	346
<i>Shoichi Hirose, Hidenori Kuwakado, and Hirotaka Yoshida</i>	

Biclique Attack on the Full HIGHT	365
<i>Deukjo Hong, Bonwook Koo, and Daesung Kwon</i>	

Preimage Attacks on Step-Reduced SM3 Hash Function	375
<i>Jian Zou, Wenling Wu, Shuang Wu, Bozhan Su, and Le Dong</i>	

Cryptographic Application

Breaking a 3D-Based CAPTCHA Scheme	391
<i>Vu Duc Nguyen, Yang-Wai Chow, and Willy Susilo</i>	

Multi-User Keyword Search Scheme for Secure Data Sharing with Fine-Grained Access Control	406
<i>Fangming Zhao, Takashi Nishide, and Kouichi Sakurai</i>	

Reaction Attack on Outsourced Computing with Fully Homomorphic Encryption Schemes	419
<i>Zhenfei Zhang, Thomas Plantard, and Willy Susilo</i>	

A Blind Digital Image Watermarking Method Based on the Dual-Tree Complex Discrete Wavelet Transform and Interval Arithmetic	437
<i>Teruya Minamoto and Ryuji Ohura</i>	

Cryptographic Protocol

On the Communication Complexity of Reliable and Secure Message Transmission in Asynchronous Networks	450
<i>Ashish Choudhury and Arpita Patra</i>	

Two-Party Round-Optimal Session-Policy Attribute-Based Authenticated Key Exchange without Random Oracles	467
<i>Kazuki Yoneyama</i>	
Sufficient Condition for Identity-Based Authenticated Key Exchange Resilient to Leakage of Secret Keys	490
<i>Atsushi Fujioka and Koutarou Suzuki</i>	
Author Index	511