Lecture Notes in Computer Science 4817

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

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

Moshe Y. Vardi
Rice University, Houston, TX, USA

Gerhard Weikum
Max-Planck Institute of Computer Science, Saarbruecken, Germany

Kil-Hyun Nam Gwangsoo Rhee (Eds.)

Information Security and Cryptology – ICISC 2007

10th International Conference
Seoul, Korea, November 29-30, 2007
Proceedings

Springer

Volume Editors

Kil-Hyun Nam
National Defense University
122-875 Susaek-dong, Eunpyung-gu, Seoul 122-875, Korea
E-mail: khnam@kndu.ac.kr

Gwangsoo Rhee
Sookmyung Women's University
52 Hyochangwon-gil, Yongsan-Ku, Seoul 140-742, Korea
E-mail: rhee@sookmyung.ac.kr

Library of Congress Control Number: 2007939824

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 3-540-76787-8 Springer Berlin Heidelberg New York
ISBN-13 978-3-540-76787-9 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 is a part of Springer Science+Business Media

springer.com

© Springer-Verlag Berlin Heidelberg 2007
Printed in Germany

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India
Printed on acid-free paper SPIN: 12192021 06/3180 5 4 3 2 1 0

Preface

ICISC 2007, the Tenth International Conference on Information Security and Cryptology, was held in Seoul, Korea, during November 29–30, 2007. It was organized by the Korea Institute of Information Security and Cryptology (KIISC) in cooperation with the Ministry of Information and Communication (MIC), Korea. 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 123 submissions from 24 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 57 prominent researchers 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 14 countries. The authors of selected papers had a few weeks to prepare final versions of their papers, aided by comments from the reviewers. The proceedings contained the revised versions of the accepted papers. However, most of these final revisions were not subject to any further editorial review.

The conference program included two invited talks from eminent researchers in information security and cryptology. The invited speakers were Daniel J. Bernstein from University of Illinois at Chicago and Mitsuru Matsui from Mitsubishi Electric Corporation.

We would like to thank everyone who contributed to the success of this conference. First, thanks to all the authors who submitted papers to this conference. Second, thanks to all 57 members of the PC listed overleaf. It was a truly nice experience to work with such talented and hard-working researchers. Third, thanks to all the external reviewers for assisting the PC in their particular areas of expertise. Fourth, we would like to thank all the participants of the conference who made this event an intellectually stimulating one through their active contribution. We would also like to thank the iChair developers in EPFL for allowing us to use their software. Finally, we are delighted to acknowledge the partial financial support provided by CIST, KISIA, NICS Tech, NITGEN, STG Security, and TSonNet.

November 2007

Kil-Huyn Nam
Gwangsoo Rhee

ICISC 2007

The 10th International Conference on
Information Security and Cryptology

November 29–30, 2007
Olympic Parktel, Seoul, Korea

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

In cooperation with
Ministry of Information and Communication (MIC), Korea
(http://www.mic.go.kr)

Organization

General Chair

Min Surp Rhee	Dankook University, Korea

Program Co-chairs

Kil-Hyun Nam	National Defense University, Korea
Gwangsoo Rhee	Sookmyung Women's University, Korea

Program Committee

Michel Abdalla	ENS and CNRS, France
Joonsang Baek	Institute for Infocomm Research, Singapore
Alex Biryukov	University of Luxembourg, Luxembourg
Bill Caelli	Queensland University of Technology, Australia
Kyo-il Chung	ETRI, Korea
Jean-Sebastien Coron	University of Luxembourg, Luxembourg
Frederic Cuppens	ENST Bretagne, France
Ed Dawson	Queensland University of Technology, Australia
Bart De Decker	Katholieke Universiteit Leuven, Belgium
Orr Dunkelman	Katholieke Universiteit Leuven, Belgium
Eduardo B. Fernandez	Florida Atlantic University, USA
Pierre-Alain Fouque	Ecole Normale Superieure, France
Mario Marques Freire	University of Beira Interior, Portugal
Marc Girault	Orange Labs, France

Philippe Golle	Palo Alto Research Center, USA
Dieter Gollmann	Hamburg University of Technology, Germany
Goichiro Hanaoka	AIST, Japan
Hiroaki Kikuchi	Tokai University, Japan
Kwangjo Kim	ICU, Korea
Christopher Kruegel	Technical University Vienna, Austria
Chi Sung Laih	National Cheng Kung University, Taiwan
Kwok-Yan Lam	Tsinghua University, China
Kristin E. Lauter	Microsoft Research, USA
Dong Hoon Lee	Korea University, Korea
Pil Joong Lee	POSTECH, Korea
Arjen K. Lenstra	EPFL, Switzerland
Yingjiu Li	Singapore Management University, Singapore
Javier Lopez	University of Malaga, Spain
Masahiro Mambo	University of Tsukuba, Japan
Mark Manulis	Ruhr University of Bochum, Germany
Keith Martin	Royal Holloway, University of London, UK
Mitsuru Matsui	Mitsubishi Electric Corporation, Japan
Atsuko Miyaji	JAIST, Japan
SangJae Moon	Kyungpook National University, Korea
Yi Mu	University of Wollongong, Australia
Jesper Buus Nielsen	University of Aarhus, Denmark
DaeHun Nyang	Inha University, Korea
Rolf Oppliger	eSECURITY Technologies, Switzerland
D'Arco Paolo	University of Salerno, Italy
Kunsoo Park	Seoul National University, Korea
Sangwoo Park	National Security Research Institute, Korea
Raphael Chung-Wei Phan	EPFL, Switzerland
Rei Safavi-Naini	University of Calgary, Canada
Kouichi Sakurai	Kyushu University, Japan
Palash Sarkar	Indian Statistical Institute, India
Dongkyoo Shin	Sejong University, Korea
Willy Susilo	University of Wollongong, Australia
Tsuyoshi Takagi	Future University, Hakodate, Japan
Jozef Vyskoc	VaF s.r.o., Slovakia
Guilin Wang	Institute for Infocomm Research, Singapore
Dongho Won	Sungkyunkwan University, Korea
Sung-Ming Yen	National Central University, Taiwan, ROC
Yongjin Yeom	National Security Research Institute, Korea
Fangguo Zhang	Sun Yat-sen University, China
Alf Zugenmaier	DoCoMo Euro-Labs, Germany

Organizing Chair

Dong-gue Park	Soonchunhyang University, Korea

Organizing Committee

Hoon Ko	Information and Communications University(ICU), Korea
DaeHun Nyang	Inha University, Korea
Jintae Oh	Electronics and Telecommunications Research Institute(ETRI), Korea
Kangbin Yim	Soonchunhyang University, Korea
Joongcheol Moon	National Security Research Institute(NSRI), Korea
Changho Seo	Kongju National University, Korea
Jaesung Kim	Korea Information Security Agency(KISA), Korea
Sangjin Kim	Korea University of Technology and Education, Korea
Sehyun Park	Chung-Ang University, Korea

External Reviewers

Imad Aad
Sultan Zayid Al-Hinai
Man Ho Au
Jean-Philippe Aumasson
Vicente Benjumea
Jean-Luc Beuchat
Annalisa De Bonis
Reinier Broker
Sebastien Canard
Ku-Young Chang
Ee-Chien Chang
Jiun-Ming Chen
Chien-Ning Chen
Wang Chih-Hung
S.Y. Chiou
Kuo-Zhe Chiou
Dickson K.W. Chiu
Yong-je Choi
Celine Coma
Nora Cuppens
Rennie deGraff
Holger Dreger
Dang Nguyen Duc
Chun-I Fan
Gerardo Fernandez
Umberto Ferraro
Ernest Foo
Georg Fuchsbauer
Soichi Furuya
D.J. Guan
JaeCheol Ha
Keisuke Hakuta
Kyusuk Han
Dong-Guk Han
Chao-Chih Hsu
Xinyi Huang
Sebastiaan Indesteege
Toshiyuki Isshiki
Tetsu Iwata
Tetsuya Izu
Ik Rae Jeong
Dimitar Jetchev
Shaoquan Jiang
Marcelo Kaihara
Nathan Keller
Dmitry Khovratovich
Jin Ho Kim
Shinsaku Kiyomoto
Hiroki Koga
Yuichi Komano
Divyan M. Konidala
Noboru Kunihiro
Wen-Chung Kuo
Eun Jeong Kwon
Yunho Lee
HoonJae Lee
Tieyan Li
Wanqing Li
Vo Duc Liem
Wei-Chih Lien
Hsi-Chung Lin
Breno de Medeiros
Anton Mityagin
Peter Montgomery
Daesung Moon
Yusuke Naito
Toshiya Nakajima
Cedric Ng
Mototsugu Nishioka
Masao Nonaka
Katsuyuki Okeya
Dag Arne Osvik
Ranjan Pal
Tae Jun Park
Maura Paterson
Kun Peng
Geong Sen Poh
Deike Priemuth-Schmid

Roberto De Prisco
Havard Raddum
Matthieu Rivain
Rodrigo Roman
Chun Ruan
Akashi Satoh
Sven Schaege
Scarlet Schwiderski-Grosche
Jae Woo Seo
Siamak F. Shahandashti
Ning Shang
Jong Hoon Shin
Masaaki Shirase
Leonie Simpson
Claudio Soriente
Chunhua Su
Hongwei Sun
Kenichi Takahashi
Terry Lam Vinh The
Julien Thomas
Jacques Traore
Jheng-Hong Tu
Yoshifumi Ueshige
Masashi Une
Ivan Visconti
Camille Vuillaume
Shuhong Wang
Baodian Wei
Christopher Wolf
Bo-Ching Wu
Yeon-Hyeong Yang
Bo-Yin Yang
Shenglin Yang
Fan Zhang
Chang-An Zhao
Xingwen Zhao
Sebastien Zimmer

Sponsoring Institutions

CIST, Korea	http://cist.korea.co.kr/
KISIA, Korea	http://www.kisia.or.kr/
NICS Tech, Korea	http://www.nicstech.com/
NITGEN, Korea	http://www.nitgen.com/
STG Security, Korea	http://www.stgsecurity.com/
TSonNet, Korea	http://www.tsonnet.co.kr/

Table of Contents

Cryptanalysis – I

Cryptanalysis of a Hash Function Proposed at ICISC 2006 1
Willi Geiselmann and Rainer Steinwandt

Cryptanalysis of Reduced Versions of the HIGHT Block Cipher from CHES 2006 11
Jiqiang Lu

A Cryptanalysis of the Double-Round Quadratic Cryptosystem 27
Antoine Scemama

Access Control

A Lightweight Privacy Preserving Authentication and Access Control Scheme for Ubiquitous Computing Environment 37
Jangseong Kim, Zeen Kim, and Kwangjo Kim

Establishing RBAC-Based Secure Interoperability in Decentralized Multi-domain Environments 49
Jinwei Hu, Ruixuan Li, and Zhengding Lu

Handling Dynamic Information Release 64
Li Jiang, Lingdi Ping, and Xuezeng Pan

Cryptanalysis – II

Improving the Time Complexity of Matsui's Linear Cryptanalysis 77
Baudoin Collard, F.-X. Standaert, and Jean-Jacques Quisquater

On Large Distributions for Linear Cryptanalysis 89
Alexander Maximov

Passive Attacks on a Class of Authentication Protocols for RFID 102
Basel Alomair, Loukas Lazos, and Radha Poovendran

Side Channel Attacks on Irregularly Decimated Generators 116
Chuan-Wen Loe and Khoongming Khoo

System Security

Asynchronous Pseudo Physical Memory Snapshot and Forensics on Paravirtualized VMM Using Split Kernel Module 131
Ruo Ando, Youki Kadobayashi, and Youichi Shinoda

Filesystem Activity Following a SSH Compromise: An Empirical Study of File Sequences 144
Jesus Molina, Xavier Chorin, and Michel Cukier

A Secure Virtual Execution Environment for Untrusted Code 156
Yan Wen and Huaimin Wang

Biometrics

Liveness Detection of Fingerprint Based on Band-Selective Fourier Spectrum 168
Changlong Jin, Hakil Kim, and Stephen Elliott

Cryptographic Protocols

Improving Upon the TET Mode of Operation 180
Palash Sarkar

Hash Functions – I

New Local Collisions for the SHA-2 Hash Family 193
Somitra Kumar Sanadhya and Palash Sarkar

Multi-collision Attack on the Compression Functions of MD4 and 3-Pass HAVAL 206
Hongbo Yu and Xiaoyun Wang

Block and Stream Ciphers

Differential Cryptanalysis of T-Function Based Stream Cipher TSC-4 ... 227
Haina Zhang and Xiaoyun Wang

New Results on Impossible Differential Cryptanalysis of Reduced AES 239
Wentao Zhang, Wenling Wu, and Dengguo Feng

Copyright Protection

A Note About the Traceability Properties of Linear Codes 251
Marcel Fernandez, Josep Cotrina, Miguel Soriano, and Neus Domingo

Smart Cards

Power Analysis Attacks on MDPL and DRSL Implementations 259
Amir Moradi, Mahmoud Salmasizadeh, and Mohammad T. Manzuri Shalmani

Safe-Error Attack on SPA-FA Resistant Exponentiations Using a HW Modular Multiplier 273
Chong Hee Kim, Jong Hoon Shin, Jean-Jacques Quisquater, and Pil Joong Lee

Elliptic Curve Cryptosystems

Generalized MMM-Algorithm Secure Against SPA, DPA, and RPA 282
Atsuko Miyaji

Pairing-Friendly Elliptic Curves with Small Security Loss by Cheon's Algorithm 297
Aya Comuta, Mitsuru Kawazoe, and Tetsuya Takahashi

Hash Functions – II

Analysis of Multivariate Hash Functions 309
Jean-Philippe Aumasson and Willi Meier

Colliding Message Pair for 53-Step HAS-160 324
Florian Mendel and Vincent Rijmen

Weaknesses in the HAS-V Compression Function 335
Florian Mendel and Vincent Rijmen

Authentication and Authorization

Security-Preserving Asymmetric Protocol Encapsulation 346
Raphael C.-W. Phan and Serge Vaudenay

Author Index 367