Lecture Notes in Computer Science 3329

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

Editorial Board

Pil Joong Lee (Ed.)

Advances in Cryptology – ASIACRYPT 2004

10th International Conference on the Theory
and Application of Cryptology and Information Security
Jeju Island, Korea, December 5-9, 2004
Proceedings

Volume Editor

Pil Joong Lee
Pohang University of Science and Technology
San 31, Hyoja-dong, Nam-gu, Pohang, Kyungbuk 790-784, Korea
On leave at KT Research Center, Seoul 137-792, Korea
E-mail: pjl@postech.ac.kr

Library of Congress Control Number: 2004115992

CR Subject Classification (1998): E.3, D.4.6, F.2.1-2, K.6.5, C.2, J.1, G.2.2

ISSN 0302-9743
ISBN 3-540-23975-8 Springer Berlin Heidelberg New York

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India
Printed on acid-free paper SPIN: 11363248 06/3142 5 4 3 2 1 0

Preface

The 10th Annual ASIACRYPT 2004 was held in Jeju Island, Korea, during December 5–9, 2004. This conference was organized by the International Association for Cryptologic Research (IACR) in cooperation with KIISC (Korean Institute of Information Security and Cryptology) and IRIS (International Research center for Information Security) at ICU (Information and Communications University), and was financially supported by MIC (Ministry of Information and Communication) in Korea.

The conference received, from 30 countries, 208 submissions that represent the current state of work in the cryptographic community worldwide, covering all areas of cryptologic research. Each paper, without the authors' information, was reviewed by at least three members of the program committee, and the papers (co-)authored by members of the program committee were reviewed by at least six members. We also blinded the reviewers' names among the reviewers until the final decision, by using pseudonyms. The reviews were then followed by deep discussions on the papers, which greatly contributed to the quality of the final selection. In most cases, extensive comments were sent to the authors.

Among 208 submissions, the program committee selected 36 papers. Two submissions were merged into a single paper, yielding the total of 35 papers accepted for presentation in the technical program of the conference. Many high-quality works could not be accepted because of the competitive nature of the conference and the challenging task of selecting a program. These proceedings contain revised versions of the accepted papers. These revisions have not been checked for correctness, and the authors bear full responsibility for the contents of their papers.

This was the first year in which the program committee selected a recipient for the Best Paper Award for the ASIACRYPT conference after lengthy discussion on its procedure and voting among program committee members. The winner of the prize for the Best Paper was Claus Diem from the University of Essen for his paper "The XL-algorithm and a Conjecture from Commutative Algebra."

The conference program included two invited lectures. Adi Shamir, from the Weizmann Institute of Science, Israel, talked on "Stream Ciphers: Dead or Alive?," and Ho-Ick Suk, the Deputy Minister for Informatization Planning at MIC of Korea, talked on "Information Security in Korea IT839 Strategy." In addition, the conference also included one rump session, chaired by Moti Yung, which featured short informal talks.

I wish to thank the program committee, whose members worked very hard over several months. I am also very grateful to the external referees who contributed with their special expertise to the selection process. Their work is highly appreciated.

The submission of all papers was received electronically using Web-based submission software which was provided by Chanathip Namprempre with modi-

fications by Andre Adelsbach. During the review process, the program committee was mainly communicated using the Web-based review software developed by Bart Preneel, Wim Moreau, and Joris Claessens.

It is my pleasure to thank the General Chair, Prof. Kwangjo Kim, for all his work in organizing the conference, and for the pleasant collaboration and various pieces of advice. In addition, I would like to extend my gratitude to the members of the local organizing committee. For financial support of the conference, the organizing committee and I gratefully acknowledge the Ministry of Information and Communication (MIC) of Korea.

I am also grateful to the secretariat of the program committee. Special thanks to Sung Ho Yoo and Young Tae Youn for maintaining both the submission server and the review server, and to Yong Ho Hwang and Yeon Hyeong Yang who served as technical assistants to the chairs and helped me with the various technical aspects of running the committee and preparing the conference proceedings, and to others for miscellaneous jobs.

Finally, we would like to thank all the other people who provided any assistance, and all the authors who submitted their papers to ASIACRYPT 2004, as well as all the participants from all over the world.

December 2004 Pil Joong Lee

ASIACRYPT 2004

December 5–9, 2004, Jeju Island, Korea

Sponsored by
International Association for Cryptologic Research (IACR)

in cooperation with
Korean Institute of Information Security and Cryptology (KIISC)
International Research Center for Information Security (IRIS) at Information and Communications University (ICU)

financially supported by
Ministry of Information and Communication (MIC) in Korea.

General Chair

Kwangjo Kim, Information and Communications University, Korea

Program Chair

Pil Joong Lee, Pohang University of Science and Technology, Korea
(on leave at KT Research Center, Korea)

Organizing Committee

Program Committee

Jee Hea An ..... SoftMax, USA
Michael Backes ..... IBM Zurich Research Lab., Switzerland
Feng Bao ..... Institute for Infocomm Research, Singapore
Colin Boyd ..... Queensland University of Tech., Australia
Liqun Chen ..... Hewlett-Packard Labs, UK
Don Coppersmith ..... IBM T.J. Watson Research Center, USA
Marc Joye ..... Gemplus, France
Jonathan Katz ..... University of Maryland, USA
Yongdae Kim ..... University of Minnesota, USA
Dong Hoon Lee ..... Korea University, Korea
Jaeil Lee ..... KISA, Korea
Arjen K. Lenstra ..... Lucent Technologies, USA and TU Eindhoven, The Netherlands
Atsuko Miyaji ..... JAIST, Japan
Jesper Buus Nielsen ..... ETH Zurich, Switzerland
Choonsik Park ..... NSRI, Korea
Dingyi Pei ..... Chinese Academy of Sciences, China
Erez Petrank ..... Technion, Israel
David Pointcheval ..... CNRS-ENS, Paris, France
Bart Preneel ..... Katholieke Universiteit Leuven, Belgium
Vincent Rijmen ..... Graz University of Technology, Austria
Bimal Roy ..... Indian Statistical Institute, India
Rei Safavi-Naini ..... University of Wollongong, Australia
Kazue Sako ..... NEC Corporation, Japan
Kouichi Sakurai ..... Kyushu University, Japan
Nigel Smart ..... University of Bristol, UK
Serge Vaudenay ..... EPFL, Switzerland
Sung-Ming Yen ..... National Central University, Taiwan
Yiqun Lisa Yin ..... Princeton University, USA
Moti Yung ..... Columbia University, USA
Yuliang Zheng ..... University of North Carolina at Charlotte, USA

Organizing Committee

Khi-Jung Ahn ..... Cheju National University, Korea
Jae Choon Cha ..... ICU, Korea
Byoungcheon Lee ..... Joongbu University, Korea
Im-Yeong Lee ..... Soonchunhyang University, Korea
Kyung-Hyune Rhee ..... Pukyong National University, Korea
Dae-Hyun Ryu ..... Hansei University, Korea

External Reviewers

Michel Abdalla
Roberto Maria Avanzi
Gildas Avoine
Joonsang Baek
Thomas Baignères
Endre Bangerter
Rana Barua
Lejla Batina
Amos Beimel
Yolanta Beres
John Black
Emmanuel Bresson
Jin Wook Byun
Christian Cachin
Qingjun Cai
Chris M. Calabro
Jan Camenisch
Ran Canetti
Christophe De Cannière
Claude Carlet
Dario Catalano
Donghoon Chang
Sanjit Chatterjee
Chien-Ning Chen
Lily Chen
Yongxi Cheng
Donghyeon Cheon
Jung Hee Cheon
Eun Young Choi
Kyu Young Choi
Kilsoo Chun
Scott Contini
Jean-Sébastien Coron
Ivan Damgård
Alex Dent
Anand Desai
Orr Dunkelman
Glenn Durfee
Matthieu Finiasz
Marc Fischlin
Caroline Fontaine
Pierre-Alain Fouque
Eiichiro Fujisaki
Jun Furukawa
Yuichi Futa
Pierrick Gaudry
Henri Gilbert
Juan González
Louis Granboulan
Robert Granger
Kishan Chand Gupta
Kil-Chan Ha
Stuart Haber
Shai Halevi
Dong-Guk Han
Helena Handschuh
Keith Harrison
Florian Hess
Yvonne Hitchcock
Christina Hoelzer
Dennis Hofheinz
Jung Yeon Hwang
Kenji Imamoto
Yuval Ishai
Ik Rae Jeong
Antoine Joux
Seok Won Jung
Pascal Junod
Markus Kaiser
Masayuki Kanda
Sungwoo Kang
Joe Kilian
Jeeyeon Kim
Jinhae Kim
Jongsung Kim
Seungjoo Kim
Yong Ho Kim
Lars Knudsen
Chiu-Yuen Koo
Jaehyung Koo
Caroline Kudla
Eyal Kushilevitz
Hidenori Kuwakado
Soonhak Kwon
Taekyoung Kwon
Mario Lamberger
Tanja Lange
Joseph Lano
Byoungcheon Lee
Changhoon Lee
Eonkyung Lee
Hoonjae Lee
Su Mi Lee
Wonil Lee
Minming Li
Yong Li
Benoît Libert
Seongan Lim
Hsi-Chung Lin
Yehuda Lindell
Yi Lu
Subhamoy Maitra
John Malone-Lee
Wenbo Mao
Keith Martin
Mitsuru Matsui
Willi Meier
Nele Mentens
Kazuhiko Minematsu
Pradeep Kumar Mishra
Chris Mitchell
Brian Monahan
Jean Monnerat
Shiho Moriai
Yi Mu
Joern Mueller-Quade
Sourav Mukhopadhyay
Hirofumi Muratani
Toru Nakanishi
Mridul Nandi
Lan Nguyen
Phong Nguyen
Masao Nonaka
Daehun Nyang
Luke O'Connor
Satoshi Obana
Wakaha Ogata
Kazuo Ohta
Takeshi Okamoto
Ivan Osipkov
Elisabeth Oswald
Dan Page

Adriana Palacio
Haeryong Park
Rafael Pass
Kenny Paterson
Olivier Pereira
Hieu Duong Phan
Benny Pinkas
Bartosz Przydatek
Michaël Quisquater
François Recher
Renato Renner
Martin Roetteler
Alon Rosen
Palash Sarkar
Katja Schmidt-Samoa
Berry Schoenmakers
Jaechul Sung
Hovav Shacham
Nicholas Sheppard
Haixia Shi
Junji Shikata
Atsushi Shimbo
Alice Silverberg
Johan Sjödin
Jung Hwan Song
Masakazu Soshi
Hirose Souichi
Martijn Stam
Ron Steinfeld
Rainer Steinwandt
Reto Strobl
Makoto Sugita
Hung-Min Sun
Soo Hak Sung
Willy Susilo
Tsuyoshi Takagi
Gelareh Taban
Mitsuru Tada
Yuko Tamura
Isamu Teranishi
Emmanuel Thomé
Eran Tromer
Shiang-Feng Tzeng
Frederik Vercauteren
Eric Verheul
Ivan Visconti
Guilin Wang
Huaxiong Wang
Shawn Wang
Bogdan Warinschi
Larry Washington
Benne de Weger
William Whyte
Christopher Wolf
Duncan Wong
Chi-Dian Wu
Hongjun Wu
Yongdong Wu
Guohua Xiong
Bo-Yin Yang
Akihiro Yamamura
Youngjin Yeom
Takuya Yoshida
Chong Zhang
Yunlei Zhao
Feng Zhu
Huafei Zhu

Table of Contents

Secure Computation

Hash Functions

Key Management

Identification

XL-Algorithms

Digital Signatures

Public Key Cryptanalysis

Invited Talk II

Symmetric Key Cryptanalysis

Protocols