

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

New York University, NY, 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

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



Springer

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

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

springeronline.com

© International Association for Cryptologic Research 2004

Printed in Germany

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

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

Table of Contents

Block Ciphers

On Feistel Ciphers Using Optimal Diffusion Mappings Across Multiple Rounds <i>Taizo Shirai, Bart Preneel</i>	1
Efficient Instantiations of Tweakable Blockciphers and Refinements to Modes OCB and PMAC <i>Phillip Rogaway</i>	16
Eliminating Random Permutation Oracles in the Even-Mansour Cipher <i>Craig Gentry, Zulfikar Ramzan</i>	32

Public Key Encryption

Towards Plaintext-Aware Public-Key Encryption Without Random Oracles <i>Mihir Bellare, Adriana Palacio</i>	48
OAEP 3-Round: A Generic and Secure Asymmetric Encryption Padding <i>Duong Hieu Phan, David Pointcheval</i>	63

Invited Talk I

Stream Ciphers: Dead or Alive? <i>Adi Shamir</i>	78
---	----

Number Theory and Algebra

On the Generalized Linear Equivalence of Functions over Finite Fields <i>Luca Breveglieri, Alessandra Cherubini, Marco Macchetti</i>	79
Sieving Using Bucket Sort <i>Kazumaro Aoki, Hiroki Ueda</i>	92
Right-Invariance: A Property for Probabilistic Analysis of Cryptography Based on Infinite Groups <i>Eonkyung Lee</i>	103

Secure Computation

Practical Two-Party Computation Based on the Conditional Gate <i>Berry Schoenmakers, Pim Tuyls</i>	119
Privacy in Non-private Environments <i>Markus Bläser, Andreas Jakobý, Maciej Liškiewicz, Bodo Manthey</i>	137
Asynchronous Proactive Cryptosystems Without Agreement <i>Bartosz Przydatek, Reto Strobl</i>	152
Lattice-Based Threshold-Changeability for Standard Shamir Secret-Sharing Schemes <i>Ron Steinfeld, Huaxiong Wang, Josef Pieprzyk</i>	170

Hash Functions

Masking Based Domain Extenders for UOWHFs: Bounds and Constructions <i>Palash Sarkar</i>	187
Higher Order Universal One-Way Hash Functions <i>Deukjo Hong, Bart Preneel, Sangjin Lee</i>	201
The MD2 Hash Function Is Not One-Way <i>Frédéric Muller</i>	214

Key Management

New Approaches to Password Authenticated Key Exchange Based on RSA <i>Muxiang Zhang</i>	230
Constant-Round Authenticated Group Key Exchange for Dynamic Groups <i>Hyun-Jeong Kim, Su-Mi Lee, Dong Hoon Lee</i>	245
A Public-Key Black-Box Traitor Tracing Scheme with Sublinear Ciphertext Size Against Self-Defensive Pirates <i>Tatsuyuki Matsushita, Hideki Imai</i>	260

Identification

- Batching Schnorr Identification Scheme with Applications to Privacy-Preserving Authorization and Low-Bandwidth Communication Devices
Rosario Gennaro, Darren Leigh, Ravi Sundaram, William Yerazunis 276
- Secret Handshakes from CA-Oblivious Encryption
Claude Castelluccia, Stanisław Jarecki, Gene Tsudik 293
- k -Times Anonymous Authentication
Isamu Teranishi, Jun Furukawa, Kazue Sako 308

XL-Algorithms

- The XL-Algorithm and a Conjecture from Commutative Algebra
Claus Diem 323
- Comparison Between XL and Gröbner Basis Algorithms
Gwénolé Ars, Jean-Charles Faugère, Hideki Imai, Mitsuru Kawazoe, Makoto Sugita 338

Digital Signatures

- Generic Homomorphic Undeniable Signatures
Jean Monnerat, Serge Vaudenay 354
- Efficient and Provably Secure Trapdoor-Free Group Signature Schemes from Bilinear Pairings
Lan Nguyen and Rei Safavi-Naini 372

Public Key Cryptanalysis

- On the Security of MOR Public Key Cryptosystem
In-Sok Lee, Woo-Hwan Kim, Daesung Kwon, Sangil Nahm, Nam-Seok Kwak, Yoo-Jin Baek 387
- Cryptanalyzing the Polynomial-Reconstruction Based Public-Key System Under Optimal Parameter Choice
Aggelos Kiayias, Moti Yung 401

Colluding Attacks to a Payment Protocol and
Two Signature Exchange Schemes
Feng Bao..... 417

Invited Talk II

Information Security in Korea IT839 Strategy
Ho-Ick Suk..... 430

Symmetric Key Cryptanalysis

How Far Can We Go Beyond Linear Cryptanalysis?
Thomas Baignères, Pascal Junod, Serge Vaudenay..... 432

The Davies-Murphy Power Attack
Sébastien Kunz-Jacques, Frédéric Muller, Frédéric Valette..... 451

Time-Memory Trade-Off Attacks on Multiplications and T -Functions
Joydip Mitra, Palash Sarkar..... 468

Cryptanalysis of Bluetooth Keystream Generator Two-Level E0
Yi Lu, Serge Vaudenay..... 483

Protocols

On Provably Secure Time-Stamping Schemes
Ahto Buldas, Märt Saarepera..... 500

Strong Conditional Oblivious Transfer and Computing on Intervals
Ian F. Blake, Vladimir Kolesnikov..... 515

Improved Setup Assumptions for 3-Round Resettable Zero Knowledge
Giovanni Di Crescenzo, Giuseppe Persiano, Ivan Visconti..... 530

Author Index..... 545