Lecture Notes in Computer Science 1163
Edited by G. Goos, J. Hartmanis and J. van Leeuwen

Advisory Board: W. Brauer D. Gries J. Stoer

Kwangjo Kim Tsutomu Matsumoto (Eds.)

Advances in Cryptology – ASIACRYPT '96

International Conference
on the Theory and Applications
of Cryptology and Information Security
Kyongju, Korea, November 3-7, 1996
Proceedings

Springer

Series Editors

Gerhard Goos, Karlsruhe University, Germany

Juris Hartmanis, Cornell University, NY, USA

Jan van Leeuwen, Utrecht University, The Netherlands

Volume Editors

Kwangjo Kim
Electronics and Telecommunications Research Institute
161 Kajong-dong, Yusong-ku, Taejon 305-350, Korea

Tsutomu Matsumoto
Division of Artificial Environment Systems and
Division of Electrical and Computer Engineering
Yokohama National University
156 Tokiwadai, Hodogaya, Yokohama 240, Japan

Cataloging-in-Publication data applied for

Die Deutsche Bibliothek - CIP-Einheitsaufnahme

Advances in cryptology : proceedings / ASIACRYPT '96, International Conference on the Theory and Applications of Cryptology and Information Security, Kyongju, Korea, November 3 - 7, 1996. Kwangjo Kim ; Tsutomu Matsumoto (ed.). - Berlin ; Heidelberg ; New York ; Barcelona ; Budapest ; Hong Kong ; London ; Milan ; Paris ; Santa Clara ; Singapore ;Tokyo : Springer, 1996
(Lecture notes in computer science ; Vol. 1163)
ISBN 3-540-61872-4
NE: Kim, Kwangjo [Hrsg.]; ASIACRYPT <1996, Kyongju>; GT

CR Subject Classification (1991): E.3-4, G.2.1, D.4.6,F.2.1-2, C.2, J.1, K.6.5, K.4.1, K.5.1-2

Mathematics Subject CLassification (1991): 94A60, 11T71, 11YXX, 68P20, 68Q20, 68Q25

ISSN 0302-9743
ISBN 3-540-61872-4 Springer-Verlag Berlin Heidelberg New York

Typesetting: Camera-ready by author
SPIN 10555455 06/3142 - 5 4 3 2 1 0 Printed on acid-free paper

Preface

ASIACRYPT'96, the conference covering all aspects of theory and applications of cryptology and information security, is held at Kyongju Hilton Hotel situated along the shore of beautiful Pomun Lake Resort in Kyongju, Korea from November 3 to 7, 1996. This is one of the Asiacrypt conferences. In the same series, ASIACRYPT'91 and ASIACRYPT'94 took place in Japan and Australia respectively. ASIACRYPT'96 is sponsored by Korea Institute of Information Security and Cryptology (KIISC), in cooperation with the International Association for Cryptologic Research (IACR) under the patronage of Ministry of Information and Communication (MIC) of Korea.

The 16-member Program Committee organized the scientific program and considered 124 submissions. Of these, 31 were accepted for presentation. The authors' affiliations of the 124 submissions and the 31 accepted papers range over 22 and 14 countries or regions, respectively. In addition, there are three invited talks by Kevin S. McCurley from Sandia National Labs., USA, Shigeo Tsujii from Chou University, Japan, and Jacques Stern from ENS, France. A Rump Session chaired by Thomas A. Berson completes the program.

The submitted version of each paper was sent to all members of the Program Committee and was extensively examined by at least three committee members and/or outside experts. The review process was rigorously blinded and the anonymity of each submission was maintained until the selection was completed. We followed the traditional policy that each member of the Program Committee could be an author of at most one accepted paper.

This is the first time the proceedings is available at the conference in the history of Asiacrypt series. These proceedings contain the revised versions of the 31 contributed talks as well as the 3 papers written by the invited speakers. Comments from the Program Committee were taken into account in the revisions. However, the authors (not the committee) bear full responsibility for the contents of their papers.

We are very grateful to the members of the Program Committee for generously spending so much of their time on the difficult task of selecting the papers. They are : Ross Anderson, Thomas A. Berson, Chin-Chen Chang, Pil Joong Lee, Mitsuru Matsui, Sang Jae Moon, David Naccache, Kaisa Nyberg, Eiji Okamoto, Paul Van Oorschot, Dingyi Pei, Bart Preneel, Moti Yung, and Yuliang Zheng. We also thank the following outside experts who assisted the Program Committee in evaluating various papers : Antoon Bosselaers, Seongtaek Chee, Joan Daemen, Seung-Cheol Goh, Sang-Geun Han, Yuji Ishizuka, Markus Jakobsson, Lars Knudsen, Sangjin Lee, Chae Hoon Lim, Françoise Levy-dit-Vehel, Masahiro Mambo, Serge Mister, Atsuko Miyaji, Hiroshi Miyano, Shiho Moriai, Tim Moses, David M'Raïhi, Takahiko Nakamura, Kazuo Ohta, Motoji Ohmori, Pascal Paillier, Sung Jun Park, Vincent Rijmen, Yasuyuki Sakai, Soo Hak Sung, Michael Wiener, and Kyung-Cheol Yang. We apologize for any omissions in this list.

We would like to appreciate all who have submitted papers to ASIACRYPT'96 and the authors of accepted and invited papers for their on-time preparation of camera-ready manuscripts.

We are pleased to thank Shin Young Lim and Seunghwa Lee for their arrangement of ASIACRYPT'96 official Web page at URL: `http://www.kreonet.re.kr/AC96/AC96.html`. Special thanks also go to Yongdae Kim and Hee Ja Kang for their help with preparation of the various tasks of program co-chairs.

Most of the work by Tsutomu Matsumoto was done while he was away from Yokohama. He would like to thank the Isaac Newton Institute of Cambridge University, U.K., Imre Mojzes of Technical University of Budapest, Hungary, and Thomas Beth of University of Karlsruhe, Germany, for providing convenient working environments.

August 1996

Kwangjo Kim
Tsutomu Matsumoto

ASIACRYPT'96

Kyongju, November 3 – 7, Korea

International Conference on the Theory and Applications of Cryptology and Information Security

Sponsored by
Korea Institute of Information Security and Cryptology (KIISC)

In cooperation with
The International Association for Cryptologic Research (IACR)

Under the patronage of
Ministry of Information and Communication (MIC), Korea

Organizing Committee

Dong Kyoo Kim (Chair, Ajou University, Korea)
Ok-Hwan Byeon (System Engineering Research Institute, Korea)
Kyung Soo Ham (Dongguk University, Korea)
Moon Seog Jun (Soon Sil University, Korea)
Kwangjo Kim (Electronics and Telecommunications Research Institute, Korea)
Kyung-Seok Lee (Korea Institute for Industrial Economics and Trade, Korea)
Sang Jae Moon (Kyungpook National University, Korea)
Kil Hyun Nam (Korea National Defense University, Korea)
Sang Kyu Park (Han Yang University, Korea)
Jae Cheol Ryou (Chung Nam National University, Korea)
Chan Shin (Korea Institute of Information Security and Cryptology, Korea)
Joo Seok Song (Yonsei University, Korea)
Chee Sun Won (Dongguk University, Korea)
Dong Ho Won (Sung Kyun Kwan University, Korea)

Contents

Cryptographic Protocols

Signature and Identification

Invited Talk 2

Visual Secret Sharing

Key Distribution

Boolean Functions

Electronic Cash 1

Electronic Cash 2

Invited Talk 3

Special Signatures

Stream Ciphers

Hard Problems