

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

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-Verlag. Violations are liable for prosecution under the German Copyright Law.

© Springer-Verlag Berlin Heidelberg 1996

Printed in Germany

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 Asiacypt 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 Asiacypt 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'Raihi, Takahiko Nakamura, Kazuo Ohta, Motoji Ohmori, Pascal Pailier, 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**

General Chair

Man Young Rhee (President of KIISC)

Program Committee

**Kwangjo Kim (Co-chair, Electronics and Telecommunications Research
Institute, Korea)**

Tsutomu Matsumoto (Co-chair, Yokohama National University, Japan)

Ross Anderson (Cambridge University, UK)

Thomas A. Berson (Anagram Laboratories, USA)

Chin-Chen Chang (National Chung Cheng University, ROC)

Pil Joong Lee (Pohang University of Science and Technology, Korea)

Mitsuru Matsui (Mitsubishi Electric Corporation, Japan)

Sang Jae Moon (Kyungpook National University, Korea)

David Naccache (Gemplus Card International, France)

Kaisa Nyberg (Finnish Defence Forces, Finland)

Eiji Okamoto (Japan Advanced Institute of Science and Technology, Japan)

Paul Van Oorschot (Bell Northern Research, Canada)

Dingyi Pei (Academia Sinica, PROC)

Bart Preneel (Katholieke Universiteit Leuven, Belgium)

Moti Yung (IBM T.J. Watson Research Center, USA)

Yuliang Zheng (Monash University, Australia)

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

Discrete Log Based Systems

A Message Recovery Signature Scheme Equivalent to DSA over Elliptic Curves	1
<i>Atsuko Miyaji (Matsushita, Japan)</i>	
Cryptographic Protocols Based on Real-Quadratic A-Fields	15
<i>Ingrid Biehl, Bernd Meyer (Univ. des Saarlandes, Germany), Christoph Thiel (Gesellschaft für Automation und Organisation, Germany)</i>	
Minding your p 's and q 's	26
<i>Ross Anderson (Cambridge Univ., UK), Serge Vaudenay (ENS, France)</i>	
Authenticated Multi-Party Key Agreement	36
<i>Mike Just (Carleton Univ., Canada), Serge Vaudenay (ENS, France)</i>	

Invited Talk 1

Cryptography and the Internet : Lessons and Challenges	50
<i>Kevin S. McCurley (Sandia National Lab., USA)</i>	

Efficient Algorithms

Generating Standard DSA Signatures Without Long Inversion	57
<i>Arjen K. Lenstra (Citibank, USA)</i>	
A Fast Software Implementation for Arithmetic Operations in $GF(2^n)$	65
<i>Erik De Win, Antoon Bosselaers, Servaas Vandenbergh, Peter De Gersen, Joos Vandewalle (Katholieke Univ. Leuven, Belgium)</i>	

Hash Function and Block Ciphers

Hash Functions Based on Block Ciphers and Quaternary Codes	77
<i>Lars Knudsen, Bart Preneel (Katholieke Univ. Leuven, Belgium)</i>	
Generalized Feistel Networks	91
<i>Kaisa Nyberg (Finnish Defence Forces, Finland)</i>	

On Applying Linear Cryptanalysis to IDEA	105
<i>Philip Hawkes (Univ. of Queensland, Australia),</i>	
<i>Luke O'Connor (Distributed Systems Technology Centre, Australia)</i>	

Cryptographic Protocols

A Multi-Recastable Ticket Scheme for Electronic Elections	116
<i>Chun-I Fan, Chin-Laung Lei (National Taiwan Univ., Taiwan)</i>	
Some Remarks on a Receipt-Free and Universally Verifiable	
Mix-Type Voting Scheme	125
<i>Markus Michels, Patrick Horster</i>	
<i>(Univ. of Technology Chemnitz-Zwickau, Germany)</i>	
Observations on Non-repudiation	133
<i>Jianying Zhou, Dieter Gollmann (Univ. of London, UK)</i>	

Signature and Identification

On the Efficiency of One-Time Digital Signatures	145
<i>Daniel Bleichenbacher (Bell Lab., USA),</i>	
<i>Ueli Maurer (ETH Zürich, Switzerland)</i>	
A Hidden Cryptographic Assumption in No-Transferable	
Identification Schemes	159
<i>Kouichi Sakurai (Kyushu Univ., Japan)</i>	

Invited Talk 2

Electronic Money and Key Management from Global and Regional	
Points of View	173
<i>Shigeo Tsujii (Chuo Univ., Japan)</i>	

Visual Secret Sharing

Limiting the Visible Space Visual Secret Sharing Schemes and	
Their Application to Human Identification	185
<i>Kazukuni Kobara, Hideki Imai (Univ. of Tokyo, Japan)</i>	

Key Distribution

Towards Characterizing When Information-Theoretic Secret Key	
Agreement Is Possible	196
<i>Ueli Maurer, Stefan Wolf (ETH Zürich, Switzerland)</i>	

Key Sharing Based on the Wire-Tap Channel Type II Concept with Noisy Main Channel	210
<i>V. Korjik, D. Kushnir</i> <i>(St. Petersburg Univ. of Telecommunications, Russia)</i>	

Boolean Functions

Generalization of Higher Order SAC to Vector Output Boolean Functions	218
<i>Kaoru Kurosawa, Takashi Satoh</i> <i>(Tokyo Institute of Technology, Japan)</i>	
On the Correlation Immune Functions and Their Nonlinearity	232
<i>Seongtaek Chee, Sangjin Lee, Daiki Lee,</i> <i>(Electronics and Telecommunications Research Institute, Korea),</i> <i>Soo Hak Sung (PaiChai Univ., Korea)</i>	

Electronic Cash 1

How to Date Blind Signatures	244
<i>Masayuki Abe, Eiichiro Fujisaki (NTT, Japan)</i>	
Provably Secure Blind Signature Schemes	252
<i>David Pointcheval, Jacques Stern (ENS, France)</i>	
Cost-Effective Payment Schemes with Privacy Regulation	266
<i>David M'Raihi (Gemplus, France)</i>	

Electronic Cash 2

Mis-representation of Identities in E-Cash Schemes and How to Prevent it	276
<i>Agnes Chan (Northeastern Univ., USA),</i> <i>Yair Frankel, Philip MacKenzie (Sandia National Lab., USA),</i> <i>Yiannis Tsiounis (Northeastern Univ, USA)</i>	
"Indirect Discourse Proofs": Achieving Efficient Fair Off-Line E-cash	286
<i>Yair Frankel (Sandia National Lab., USA), Yiannis Tsiounis</i> <i>(Northeastern Univ, USA), Moti Yung (IBM, USA)</i>	

Invited Talk 3

The Validation of Cryptographic Algorithms	301
<i>Jacques Stern (ENS, France)</i>	

Special Signatures

Convertible Group Signatures	311
<i>Seung Joo Kim (Sung Kyun Kwan Univ., Korea), Sung Jun Park (KISA, Korea), Dong Ho Won (Sung Kyun Kwan Univ., Korea)</i>	
How to Utilize the Transformability of Digital Signatures for Solving the Oracle Problem	322
<i>Masahiro Mambo (JAIST, Japan), Kouichi Sakurai (Kyushu Univ., Japan), Eiji Okamoto (JAIST, Japan)</i>	
On the Risk of Disruption in Several Multiparty Signature Schemes	334
<i>Markus Michels, Patrick Horster (Univ. of Technology Chemnitz-Zwickau, Germany)</i>	

Stream Ciphers

Correlation Attacks on Cascades of Clock Controlled Shift Registers	346
<i>Willi Geiselmann (Univ. of Karlsruhe, Germany), Dieter Gollmann (Univ. of London, UK)</i>	
Conditional Correlation Attack on Nonlinear Filter Generators	360
<i>Sangjin Lee, Seongtaek Chee, Sangjoon Park, Sungmo Park (Electronics and Telecommunications Research Institute, Korea)</i>	

Hard Problems

The Cryptographic Security of the Syndrome Decoding Problem for Rank Distance Codes	368
<i>Florent Chabaud, Jacques Stern (ENS, France)</i>	
A World Wide Number Field Sieve Factoring Record: on to 512 Bits	382
<i>James Cowie (Cooperating Systems Co., USA), Bruce Dodson (Lehigh Univ., USA), R. Marije Elkenbracht-Huizing (Centrum voor Wiskunde en Informatica, The Netherlands), Arjen K. Lenstra (Citibank, USA), Peter L. Montgomery (USA), Jörg Zayer (Germany)</i>	

Author Index	395
--------------------	-----