

Josef Pieprzyk
Reihanah Safavi-Naini (Eds.)

Advances in Cryptology – ASIACRYPT '94

4th International Conference on
the Theory and Applications of Cryptology
Wollongong, Australia
November 28 - December 1, 1994
Proceedings



Springer

Lecture Notes in Computer Science

917

Edited by G. Goos, J. Hartmanis and J. van Leeuwen

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

Series Editors

Gerhard Goos

Universität Karlsruhe

Vincenz-Priessnitz-Straße 3, D-76128 Karlsruhe, Germany

Juris Hartmanis

Department of Computer Science, Cornell University

4130 Upson Hall, Ithaca, NY 14853, USA

Jan van Leeuwen

Department of Computer Science, Utrecht University

Padualaan 14, 3584 CH Utrecht, The Netherlands

Volume Editors

Josef Pieprzyk

Reihanah Safavi-Naini

Department of Computer Science, The University of Wollongong

Wollongong, N.S.W. 2500, Australia

CR Subject Classification (1991):E.3-4, G.2.1, C.2.0, F.2.2

1991 Mathematics Subject Classification: 68P25, 94A60, 11T71

ISBN 3-540-59339-X Springer-Verlag Berlin Heidelberg New York

CIP data applied for

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 1995

Printed in Germany

Typesetting: Camera-ready by author

SPIN: 10485870 06/3142-543210 - Printed on acid-free paper

PREFACE

The ASIACRYPT'94 was the fourth conference in the Asia-Pacific region and was a continuation of AUSCRYPT'90, ASIACRYPT'91 and AUSCRYPT'92 series of workshops devoted to the Theory and Application of Cryptology. The conference was held on the campus of the University of Wollongong, New South Wales, Australia. It started on November 28, 1994 and ended on December 1, 1994. The conference was organized by the Center for Computer Security Research and the Department of Computer Science, University of Wollongong, in co-operation with the International Association for Cryptologic Research (IACR). The sponsor of the conference was the Center for Computer Security Research, University of Wollongong.

The conference ran very smoothly and with a relaxed atmosphere. The credit for this goes to the General Chair, Professor Jennifer Seberry of the University of Wollongong, Mrs Margot Hall (the Conference Secretary) and graduate students of the Department of Computer Science.

The Program Chair received 99 submissions from 20 countries. The Program Committee reviewed 94 papers - the remaining five were not considered as they arrived too late. After a rigorous blind review process, 30 papers were accepted. Program Committee members' submissions were anonymous and went through exactly the same refereeing procedure as all other papers. From the accepted papers, Japan has 8, Australia 6, USA 3, France and Israel 2 each, and China, Finland, Germany, Korea, New Zealand, Saudi Arabia, Spain, UK, Yugoslavia a single paper each. The Committee chose three invited speakers: Thomas Beth, the Director of European Institute for System Security, University of Karlsruhe, Germany, Catherine Meadows, Center for High Assurance Computer Systems, Naval Research Laboratory, USA, and Hideki Imai, Institute of Industrial Science, University of Tokyo, Japan. These invited talks were not refereed and the authors bear full responsibility for their contents.

The traditional Rump Session was organized by Dr Reihanah Safavi-Naini with the help of Bill Forsyth. There were 13 submissions, all of which were presented. After a review 4 of them were accepted and placed in the proceedings.

We are pleased to thank all the members of the Program Committee: Don Beaver (Pennsylvania State University, USA), Eli Biham (Technion, Israel), Chin-Chen Chang (Chung Cheng University, Taiwan), Zong-Duo Dai (Academia Sinica, PROC), Yvo Desmedt (University of Wisconsin, USA), Toshiya Itoh (Tokyo Institute of Technology, Japan), Tsutomu Matsumoto (Yokohama National University, Japan), Andrew Odlyzko (AT&T Bell Laboratories, USA), Tatsuaiki

Okamoto (NTT, Japan), Bart Preneel (Katholieke Universiteit Leuven, Belgium), Rainer Rueppel (R^3 Security Engineering AG, Switzerland), Yuliang Zheng (University of Wollongong, Australia). Thanks also go to the reviewers nominated by Program Committee members.

The conference also gave an opportunity for participants from Australia and New Zealand to get together and establish the Australasian Society for Electronic Security (ASES). The aim of ASES are to promote research and development in all areas of information security in the region.

We wish to thank all the authors for sending their submissions (successful or otherwise), the speakers, and all the participants of Asiacrypt'94 conference.

Wollongong, New South Wales, Australia
January 1995

Josef Pieprzyk
Reihanah Safavi-Naini

ASIACRYPT'94

THE 4th CONFERENCE ON THE THEORY AND
APPLICATIONS OF CRYPTOLOGY

Sponsored by

**Center for Computer Security Research
University of Wollongong, Australia**

In co-operation with

**The International Association for Cryptologic Research
(IACR)**

General Chair

Jennifer Seberry

(University of Wollongong, Australia)

Program Chair

Josef Pieprzyk

(University of Wollongong, Australia)

Program Committee

Donald Beaver

(Pennsylvania State University, USA)

Eli Biham

(Technion, Israel)

Chin-Chen Chang

(Chung-Cheng University, Taiwan)

Zong-Duo Dai

(Academia Sinica, PROC)

Yvo Desmedt

(University of Wisconsin-Milwaukee, USA)

Toshiya Itoh

(Tokyo Institute of Technology, Japan)

Tsutomu Matsumoto

(Yokohama National University, Japan)

Andrew Odlyzko

(AT&T Bell Laboratories, USA)

Tatsuaki Okamoto

(NTT, Japan)

Bart Preneel

(Katholieke Universiteit Leuven, Belgium)

Rainer Rueppel

(R³ Security Engineering AG, Switzerland)

Reihanah Safavi-Naini

(University of Wollongong, Australia)

Yuliang Zheng

(University of Wollongong, Australia)

Referees

Ross Anderson (*Cambridge University*), Donald Beaver (*Pennsylvania State University*), Amos Beimel (*Technion*), Charles Bennett (*IBM Watson Research Center*), Eli Biham (*Technion*), Mike Burmester (*University of London*), Chin-Chen Chang (*Chung-Cheng University*), Yvo Desmedt (*University of Wisconsin-Milwaukee*), Toshiya Itoh (*Tokyo Institute of Technology*), Kaoru Kurosawa (*Tokyo Institute of Technology*), Xuejia Lai (*R³ Security Engineering AG*), Keith Martin (*University of Adelaide*), Tsutomu Matsumoto (*Yokohama National University*), Yi Mu (*University of Wollongong*), Andrew Odlyzko (*AT&T Bell Laboratories*), Tatsuaki Okamoto (*NTT*), Josef Pieprzyk (*University of Wollongong*), Bart Preneel (*Katholieke Universiteit Leuven*), Jim Reeds (*AT&T Bell Laboratories*), Rainer Rueppel (*R³ Security Engineering AG*), Reihanah Safavi-Naini (*University of Wollongong*), Peter Shor (*AT&T Bell Laboratories*), Yuliang Zheng (*University of Wollongong*).

Organizing Committee (*all from University of Wollongong, Australia*)

Margot Hall (*Conference Secretary*), Mark Arnold, Shahram Bakhtiari, Ahmad Baraani-Dastjerdi, Ghulam Rasool Chaudhry, Nitin Devikar, Mansour Esmaili, Bill Forsyth, Hossein Ghodosi, Justin Lister, Anish Mathuria, Viswanathan Narain, Colin Spargo

CONTENTS

Invited Lecture 1:

- Multifeature security through homomorphic encryption 1
T. Beth (Universität Karlsruhe, Germany)

Session 1: SECRET SHARING

Chair: E. Dawson

- Multiplicative non-abelian sharing schemes and their application
to threshold cryptography 21
*Y. Desmedt (University of Wisconsin-Milwaukee, USA),
G. Di Crescenzo (Università di Salerno, Italy), and
M. Burmester (University of London, UK)*
- Lower bound on the size of shares of nonperfect secret sharing schemes 33
K. Okada and K. Kurosawa (Tokyo Institute of Technology, Japan)
- On sharing many secrets 42
*W.-A. Jackson, K.M. Martin, and C.M. O'Keefe
(University of Adelaide, Australia)*
- Combinatorial interpretation of secret sharing schemes 55
K. Kurosawa and K. Okada (Tokyo Institute of Technology, Japan)

Session 2: STREAM CIPHERS

Chair: E. Biham

- A correlation attack on the binary sequence generators
with time-varying output function 67
M.J. Mihaljević (Academy of Arts and Sciences, Yugoslavia)
- On the linear complexity of nonlinearly filtered PN-sequences 80
*A. Fúster-Sabater (Institute of Electronics of Communications, Spain) and
P. Caballero-Gil (University of La Laguna, Spain)*
- Intrinsic statistical weakness of keystream generators 91
J.Dj. Golić (Queensland University of Technology, Australia)

Session 3: CRYPTOGRAPHIC FUNCTIONS

Chair: Z.-D. Dai

Semi-bent functions 107
S. Chee, S. Lee, and K. Kim
(Electronics and Telecommunications Research Institute, Korea)

Structures of cryptographic functions with
 strong avalanche characteristics 119
J. Seberry, X.-M. Zhang, and Y. Zheng
(University of Wollongong, Australia)

Invited Lecture 2:

Formal verification of cryptographic protocols: a survey 133
C.A. Meadows (Naval Research Laboratory, USA)

Session 4: PROTOCOLS

Chair: D. Beaver

Efficient electronic money 153
Y. Yacobi (Bellcore, USA)

How to prevent buying of votes in computer elections 164
V. Niemi (University of Vaasa, Finland) and
A. Renvall (University of Turku, Finland)

Design and analysis of key exchange protocols
 via secure channel identification 171
C. Boyd and W. Mao (University of Manchester, UK)

Zero-knowledge proofs of computational power
 in the shared string model 182
A. De Santis (Università di Salerno, Italy),
T. Okamoto (NTT Laboratories, Japan), and
G. Persiano (Università di Catania, Italy)

Invited Lecture 3:

Information security aspects of spread spectrum systems 193
H. Imai (University of Tokyo, Japan)

Session 5: AUTHENTICATION AND DIGITAL SIGNATURES

Chair: J. Golić

Combinatorial structure of A-codes with r-fold security 211
R. Safavi-Naini and L. Tombak (University of Wollongong, Australia)

Meta-message recovery and meta-blind signature schemes based on
 the discrete logarithm problem and their applications 224
P. Horster, M. Michels, and H. Petersen
(University of Technology Chemnitz-Zwickau, Germany)

A digital signature scheme based on linear error-correcting
 block codes 238
M. Alabbadi (KACST, Saudi Arabia) and
S.B. Wicker (Georgia Tech - Lorraine, France)

Secure acceleration of DSS signatures using insecure server 249
P. Béguin (Ecole Normale Supérieure, France) and
J.-J. Quisquater (Université Catholique de Louvain, Belgium)

Session 6: CRYPTANALYSIS

Chair: L. O'Connor

The magic words are squeamish ossifrage 263
D. Atkins (Cambridge, USA), M. Graff (Iowa State University, USA),
A.K. Lenstra (Bellcore, USA), and P.C. Leyland (Oxford University, UK)

Cryptanalysis of multiple modes of operation 278
E. Biham (Technion, Israel)

Linear cryptanalysis of LOKI and s^2 DES 293
T. Tokita, T. Sorimachi and M. Matsui
(Mitsubishi Electric Corporation, Japan)

Session 7: HASH FUNCTIONS

Chair: T. Matsumoto

Collisions and inversions for Damgård's whole hash function 307
J. Patarin (Bull CP8, France)

Attacking the SL_2 hashing scheme 322
C. Charnes and J. Pieprzyk (University of Wollongong, Australia)

Session 8: KEY DISTRIBUTION

Chair: T. Okamoto

Security of the center in key distribution schemes 333
K. Kurosawa, K. Okada (Tokyo Institute of Technology, Japan), and
K. Sakano (Matsushita Electric Industrial Co., Japan)

Incidence Structures for Key Sharing 342
T. Matsumoto (Yokohama National University, Japan)

Session 9: PUBLIC KEY CRYPTOGRAPHY

Chair: Y. Zheng

A public-key cryptosystem and a digital signature system based on
 the Lucas function analogue to discrete logarithms 357
P. Smith (LUC Encryption Technology, New Zealand) and
C. Skinner (LUC Encryption Technology, Australia)

Higher radix nonrestoring modular multiplication algorithm and
public-key LSI architecture with limited hardware resources365
M. Abe and H. Morita (NTT, Japan)

Low exponent attack against elliptic curve RSA 376
*K. Kurosawa, K. Okada (Tokyo Institute of Technology, Japan), and
S. Tsujii (Chuo University, Japan)*

Session 10: BLOCK CIPHER ALGORITHMS

Chair: R. Safavi-Naini

A unified Markov approach to differential and linear cryptanalysis 387
L. O'Connor and J.Dj. Golić
(Queensland University of Technology, Australia)

How to strengthen DES using existing hardware398
E. Biham and A. Biryukov (Technion, Israel)

Rump Session

Chair: R. Safavi-Naini

Some cryptographic properties of exponential functions 415
*X. Chang (University of Science and Technology, China),
Z.-D. Dai (Academia Sinica, China), and
G. Gong (University of Chengdu, China)*

Factoring: the DNA solution 419
D. Beaver (Penn State University, USA)

Can one design a signature scheme based on error-correcting codes ?424
J. Stern (Ecole Normale Supérieure, France)

DESV-1: a variation of the data encryption standard (DES) 427
G. Carter, A. Clark, and L. Nielsen
(Queensland University of Technology, Australia)

Author Index 431