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

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

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), Tatsuaki

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	*(R^3 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 *(R^3 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 *(R^3 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