Lecture Notes in Computer Science

Edited by G. Goos and J. Hartmanis

453

J. Seberry J. Pieprzyk (Eds.)

Advances in Cryptology – AUSCRYPT '90

International Conference on Cryptology
Sydney, Australia, January 8–11, 1990
Proceedings

Springer-Verlag
Berlin Heidelberg New York London
Paris Tokyo Hong Kong Barcelona

Editors

Jennifer Seberry
Josef Pieprzyk
Department of Computer Science, University College
The University of New South Wales
Australian Defence Force Academy
Canberra, ACT 2600, Australia

CR Subject Classification (1987): E.3

ISBN 3-540-53000-2 Springer-Verlag Berlin Heidelberg New York
ISBN 0-387-53000-2 Springer-Verlag New York Berlin Heidelberg

Printing and binding: Druckhaus Beltz, Hemsbach/Bergstr.
2145/3140-543210 – Printed on acid-free paper

AUSCRYPT'90

A Workshop on the Theory and Application of Cryptographic Techniques

January 8-11, 1990

The University of New South Wales, Sydney

Sponsored by

The International Association for Cryptologic Research

in cooperation with

The IPACE Institute at UNSW

and

Department of Computer Science, University College, ADFA

Centre for Communication Security Research

General Chair: Jennifer Seberry, The University of NSW, Canberra, Australia

Program Chairs: Josef Pieprzyk, The University of NSW, Canberra, Australia
Rainer Rueppel, Crypto AG, Zug, Switzerland
Scott Vanstone, University of Waterloo, Waterloo, Canada

Program Committee:

Gordon Agnew, University of Waterloo, Waterloo, Canada
Ingemar Ingemarsson, University of Linkoping, Linkoping. Sweden
Ron Mullin, University of Waterloo, Waterloo, Canada
Wyn Price, National Physical Laboratory, Teddington, United Kingdom
Rei Safavi-Naini, The University of NSW, Canberra, Australia

PREFACE

This book is the proceedings of AUSCRYPT '90, the first conference sponsored by the International Association for Cryptological Research to be held in the southern hemisphere and the first outside the EUROCRYPT series held in European countries each northern spring and the CRYPTO series held in Santa Barbara, USA each August.

The proceedings from these earlier conferences have been published in the Springer-Verlag Lecture Notes in Computer Science series since 1986.

Papers in this volume are organized into eleven sections. The first ten sections comprise all of the papers on the regular program, including a few papers on the program which, unfortunately, were not presented at the meeting. The last section contains some of the papers presented at the "Rump Session" organized by Josef Pieprzyk.

AUSCRYPT '90 was attended by 95 people representing sixteen countries.

For the first time a skills workshop was held the day before the conference, with such eminent cryptographers as D. Gollmann (West Germany), I. Ingemarsson (Sweden), K. Ohta (Japan), R. Rueppel (Switzerland) and S. Vanstone (Canada) teaching in the area of their expertise. J. Seberry represented Australia at this event. Forty-one people attended the workshop.

It gives us great pleasure to express our thanks here to the members of the program committee: Dr R. Rueppel, Dr W.Price, and Dr I. Ingemarsson from Europe; Dr S. Vanstone, Dr R. Mullin, and Dr G. Agnew from North America; and Dr R. Safavi-Naini, and the other members of the Centre for Computer Security Research, for the rest of the world. They were all efficient, pleasant and wonderful co-workers.

Local organization was arranged by Ms C. Burke of the IPACE Institute, on the Sydney campus of The University of NSW. The conference dinner was held on a ferry on Sydney Harbour and was a spectacular success.

Many thanks to all the members of the Centre for Computer Security Research: Dr R. Safavi-Naini; Mr L. Brown; Ms L. Condie; Mr T. Hardjono; Mrs C. Newberry; Mr M. Newberry; Mr D. Rubie; Mrs E. Trott and Mrs E. Tait, all of whom readily worked at every task they were given to make the conference function smoothly and ensure its scientific success.

This conference was made possible by the support of the International Association for Cryptologic Research, The Centre for Computer Security Research, Prentice Hall Pty Ltd, and Telecom Australia.

Jennifer Seberry
Josef Pieprzyk

CONTENTS

SECTION 5: PSEUDORANDOMNESS AND SEQUENCES II

SECTION 6: BLOCK CIPHERS

SECTION 7: ZERO-KNOWLEDGE PROTOCOLS

SECTION 8: THEORY

SECTION 9: APPLICATIONS

SECTION 10: IMPLEMENTATIONS

SECTION 11: RUMP SESSION