Lecture Notes in Computer Science

Edited by G. Goos and J. Hartmanis

293

Carl Pomerance (Ed.)

Advances in Cryptology — CRYPTO '87

Proceedings

Springer-Verlag

Berlin Heidelberg New York London Paris Tokyo

Editorial Board

D. Barstow W. Brauer P. Brinch Hansen D. Gries D. Luckham
C. Moler A. Pnueli G. Seegmüller J. Stoer N. Wirth

Editor

Carl Pomerance
Department of Mathematics, The University of Georgia
Athens, Georgia 30602, USA

CR Subject Classification (1987): E.3

ISBN 3-540-18796-0 Springer-Verlag Berlin Heidelberg New York
ISBN 0-387-18796-0 Springer-Verlag New York Berlin Heidelberg

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 other ways, and storage in data banks. Duplication of this publication or parts thereof is only permitted under the provisions of the German Copyright Law of September 9, 1965, in its version of June 24, 1985, and a copyright fee must always be paid. Violations fall under the prosecution act of the German Copyright Law.

© Springer-Verlag Berlin Heidelberg 1988
Printed in Germany

Printing and binding: Druckhaus Beltz, Hemsbach/Bergstr.
2145/3140-543210

Preface

This book is the proceedings of CRYPTO'87, one in a series of annual conferences devoted to cryptologic research. For citations of proceedings of CRYPTO and Eurocrypt conferences before 1986, see

Advances in Cryptology-CRYPTO'86 Proceedings, A. M. Odlyzko, ed., Lecture Notes in Computer Science #263, Springer, 1987.

Papers in this volume are organized into seven sections. The first six sections comprise all of the papers on the regular program, including two papers on the program that unfortunately were not presented at the meeting. The seventh section contains some of the papers presented at the "Rump Session" organized by W. Diffie and also includes a short note by T. R. N. Rao which comments on the paper of R. Struik and J. van Tilburg.

CRYPTO'87 was attended by 170 people representing 19 countries. Responsible not only for the conference as a whole, G. B. Agnew also took care of local arrangements in Santa Barbara. We all owe him a debt of gratitude for his highly successful efforts.

It is my special pleasure to thank my fellow members of the Program Committee: T. A. Berson, E. F. Brickell, A. M. Odlyzko, and G. J. Simmons. They all were most prompt, efficient, and willing to cheerfully compromise on disagreements. My task would have been hopeless without them.

I also would like to thank the authors and attendees who made CRYPTO'87 such a success. Special thanks are due to University of Georgia secretaries D. Byrd and P. Sisk and L. B. Montz at Springer for their help in the production of this volume.

Athens, Georgia

Carl Pomerance

CRYPTO'87

A Conference on the Theory and Applications of Cryptographic Techniques

held at the University of California, Santa Barbara,
through the cooperation of the
Computer Science Department

August 16-20, 1987

sponsored by:

The International Association for Cryptologic Research

in cooperation with

The IEEE Computer Society Technical Committee
On Security and Privacy

ORGANIZERS

General Chairman: G. B. Agnew (U. Waterloo)

Program Committee:
T. A. Berson (Anagram Laboratories)
E. F. Brickell (Bell Communications Research)
A. M. Odlyzko (AT&T Bell Laboratories)
C. Pomerance (U. Georgia, Chairman)
G. J. Simmons (Sandia National Laboratories)

TABLE OF CONTENTS

SECTION 1: COMMUNICATION NETWORKS AND STANDARDS

SECTION 2: PROTOCOLS

SECTION 3: KEY DISTRIBUTION SYSTEMS

SECTION 4: PUBLIC KEY SYSTEMS

SECTION 5: DESIGN AND ANALYSIS OF CRYPTOGRAPHIC SYSTEMS

SECTION 6: APPLICATIONS

SECTION 7: INFORMAL CONTRIBUTIONS