Lecture Notes in Computer Science

Edited by G. Goos and J. Hartmanis

330

Christoph G. Günther (Ed.)

Advances in Cryptology – EUROCRYPT '88

Workshop on the Theory and Application of Cryptographic Techniques
Davos, Switzerland, May 25–27, 1988
Proceedings

Springer-Verlag
Berlin Heidelberg New York London Paris Tokyo

Editor

Christoph G. Günther
Asea Brown Boveri, Corporate Research
CH-5405 Baden, Switzerland

CR Subject Classification (1987): D.4.6, E.3, H.2.0

ISBN 3-540-50251-3 Springer-Verlag Berlin Heidelberg New York
ISBN 0-387-50251-3 Springer-Verlag New York Berlin Heidelberg

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

PREFACE

The International Association for Cryptologic Research (IACR) organizes two international conferences every year, one in Europe and one in the United States. EUROCRYPT'88, held in the beautiful environment of the Swiss mountains in Davos, was the sixth European conference. The number of contributions and of participants at the meeting has increased substantially, which is an indication of the high interest in cryptography and system security in general.

The interest has not only increased but has also further moved towards authentication, signatures and other protocols. This is easy to understand in view of the urgent needs for such protocols, in particular in connection with open information systems, and in view of the exciting problems in this area. The equally fascinating classical field of secrecy, *i.e.* the theory, design and analysis of stream or block ciphers and of public key cryptosystems, was however also well represented and several significant results were communicated.

The present proceedings contain all contributions which were accepted for presentation. The chapters correspond to the sessions at the conference.

I am grateful to all authors of these contributions for the careful preparation and prompt submission of their papers. On behalf of the General Chairman, it is a pleasure to thank the authors and the members of the Program Committee for having made the conference such an interesting and stimulating meeting. We are indebted to the sponsors for their generous donations and to the members of the Organization Committee, who have so perfectly organized the meeting.

Baden, June 1988 C.G.G.

EUROCRYPT'88

was sponsored by the

International Association for Cryptologic Research (IACR)

General Chairman: James L. Massey, Swiss Federal Institute of Technology, Zürich, Switzerland

Program Chairman: Ingemar Ingemarsson, Linköping University, Sweden

Organizing Committee:

José Clarinval, Zürich
Christoph G. Günther, Baden
Kirk H. Kirchhofer, Zug
Ueli Maurer, Zürich
Rainer A. Rueppel, Zug
Paul Schoebi, Regensdorf
Thomas Siegenthaler, Zürich
Othmar Staffelbach, Regensdorf

Program Committee:

Rolf Blom, Stockholm
Lennart Brynielsson, Stockholm
Ivan Damgård, Aarhus
Viveke Fåk, Linköping
Tor Helleseth, Bergen
Rolf Johannesson, Lund

The conference was generously supported by

Union Bank of Switzerland, Zürich
Springer-Verlag, Heidelberg and New York
Amstein Walthert Kleiner AG, Zürich, Switzerland
Asea Brown Boveri AG, Zürich, Switzerland
Ascom-Radiocom AG, Solothurn, Switzerland
Crypto AG, Zug, Switzerland
Gretag Ltd., Regensdorf, Switzerland