Lecture Notes in Computer Science 547
Edited by G. Goos and J. Hartmanis

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

D. W. Davies (Ed.)

Advances in Cryptology– EUROCRYPT '91

Workshop on the Theory and Application of Cryptographic Techniques
Brighton, UK, April 8-11, 1991
Proceedings

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

Series Editors

Gerhard Goos
GMD Forschungsstelle
Universität Karlsruhe
Vincenz-Priessnitz-Straße 1
W-7500 Karlsruhe, FRG

Juris Hartmanis
Department of Computer Science
Cornell University
Upson Hall
Ithaca, NY 14853, USA

Volume Editor

Donald W. Davies
Royal Holloway and Bedford New College, Univ. of London
Egham Hill, Surrey TW 20 0EX, UK

CR Subject Classification (1991): E.3-4, D.4.6, H.2.0, G.2.1

ISBN 3-540-54620-0 Springer-Verlag Berlin Heidelberg New York
ISBN 0-387-54620-0 Springer-Verlag New York Berlin Heidelberg

Typesetting: Camera ready by author
Printing and binding: Druckhaus Beltz, Hemsbach/Bergstr.
45/3140-543210 - Printed on acid-free paper

Preface

A series of open workshops devoted to modern cryptology began in Santa Barbara, California in 1981 and was followed in 1982 by a European counterpart in Burg Feurstein, Germany. The series has been maintained with summer meetings in Santa Barbara and spring meetings somewhere in Europe. At the 1983 meeting in Santa Barbara the International Association for Cryptologic Research was launched and it now sponsors all the meetings of the series.

Following the tradition of the series, papers were invited in the form of extended abstracts and were reviewed by the programme committee, which selected those to be presented. After the meeting, full papers were produced, in some cases with improvements and corrections. These papers form the main part of the present volume. They are placed in the same order that they took at the meeting and under the same headings, for ease of reference by those who attended. The classification under these headings was a little arbitary, needing to fit the timing of the day's activities, but it makes a workable method of arrangement.

Also following tradition, a "rump session" was held during one evening, under the effective chairmanship of John Gordon. These were short presentations and those present found them to have some real interest, therefore we have taken the unusual step of including short papers contributed by the rump session speakers at the end of this volume, with a necessarily simplified review process.

There was no attempt by the programme committee to guide the programme towards particular themes, though the interests of the committee members may have influeced the shape of the meeting. In our admittedly rough classification the biggest group was about sequences, the term interpreted rather widely. The next biggest group concerned cryptanalysis, which was welcomed because cryptanalysis is the criterion by which algorithms and protocols in cryptography must be judged.

Zero-knowledge interactive protocols figured less this year than at earlier meetings - a consequence of the submissions we received, not of policy.

Smaller groups of papers dealt with S-box criteria, signatures and new ideas in public key cryptography. Then there were many papers placed into sessions labelled "theory" and "applications".

My task as programme chair was made easier by the high quality of papers we received, though we regretted having to reject some of the papers because of time limitations. I would like to thank the programme committee for its hard work of reviewing papers and the organizing committee for ensuring that everything ran smoothly, including the social events. Then, of course, the authors deserve many thanks for favouring Eurocrypt '91 with the publication of their excellent work and for preparing their final papers with (in most cases) admirable despatch.

London, August 1991 Donald W. Davies

EUROCRYPT '91

General Chairman:
Andrew J. Clark
(Logica Aerospace and Defence Ltd.)

Organizing Committee:
Keith Martin
(Royal Holloway and Bedford New College, Univ. of London)
Martin Meikle-Small (Aspen Consultants)
Ben Meisner (RHBNC)
Kathleen Quinn (RHBNC)
Matthew Robshaw (RHBNC)

Program Chairman:
Donald W. Davies (RBHNC)

Program Committee:
Thomas Beth (Univ. of Karlsruhe)
Colin Boyd (Univ. of Manchester)
Norbert Cot (EHEI Université, Paris)
Viveke Fåk (Linköping University)
John Gordon (Cybermation Limited)
Siegfried Herda (GMD, Germany)
Arjen Lenstra (Bellcore, NJ)
Tsutomu Matsumoto (Yokohama National Univ.)
Fred Piper (RHBNC)
Claus Schnorr (Universität Frankfurt)

EUROCRYPT '91 was sponsored by:
International Association for Cryptologic Research (IACR)
in association with:
Logica Aerospace and Defence Limited
ABN Bank
Coopers and Lybrand Deloitte
Northern Telecom
with additional support from:
Computer Security Limited
IBM United Kingdom Limited

Contents

Sequences II

Sequences III

Signatures

Theory I

Theory II

S-Box Criteria

Applications I

Applications II

Public Key Cryptography

Short Papers presented at the "Rump Session"