Lecture Notes in Computer Science

Edited by G. Goos and J. Hartmanis

218

Advances in Cryptology – CRYPTO '85

Proceedings

Edited by Hugh C. Williams

Springer-Verlag
Berlin Heidelberg New York Tokyo

Editor

Hugh C. Williams
Department of Computer Science, University of Manitoba
Winnipeg, Manitoba R3T 2N2, Canada

CR Subject Classifications (1985): E.3

ISBN 3-540-16463-4 Springer-Verlag Berlin Heidelberg New York Tokyo
ISBN 0-387-16463-4 Springer-Verlag New York Heidelberg Berlin Tokyo

CIP-Kurztitelaufnahme der Deutschen Bibliothek. Advances in cryptology: proceedings of CRYPTO ... – Berlin; Heidelberg; New York; Tokyo: Springer.
Teilw. in d. Vorlage auch: Workshop on the Theory and Application of Cryptograph. Techniques
NE: CRYPTO 1985 (1986).
(Lecture notes in computer science: Vol. 218)
ISBN 3-540-16463-4 (Berlin ...)
ISBN 0-387-16463-4 (New York ...
NE: GT

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

Preface

In the summer of 1981 Allen Gersho organized the first major open conference ever devoted to cryptologic research. This meeting, Crypto '81, was held at the University of California campus in Santa Barbara. Since then the Crypto' conference has become an annual event. These are the proceedings of the fifth[1] of these conferences, Crypto '85.

Each section of this volume corresponds to a session at the meeting. The papers were accepted by the program committee, sometimes on the basis of an abstract only, and appear here without having been otherwise refereed. The last section contains papers for some of the impromptu talks given at the traditional rump session. Each of these papers was refereed by a single member of the program committee. An author index as well as a keyword index, the entries for which were mainly supplied by the authors, appear at the end of the volume.

Unfortunately, two of the papers accepted for presentation at Crypto '85 could not be included in this book they are:

Unique Extrapolation of Polynomial Recurrences
J.C. Lagarias and J.A. Reeds (A.T. & T Bell Labs)

Some Cryptographic Applications of Permutation Polynomials and Permutation Functions
Rupert Nöbauer (Universität für Bildungswissenschaften, Austria)

It is my great pleasure to acknowledge the efforts of all of those who contributed to making these proceedings possible: the authors, program committee, other organizers of the meeting, IACR officers and directors, and all the attendees. I would also like to thank Lynn Montz of Springer-Verlag for her patient assistance in preparing this volume.

Winnipeg, Manitoba, Canada *H.C.W.*
January 1986

[1] Proceedings of the other Crypto conferences have also been published. The interested reader can find these listed in the preface of Advances in Cryptology 84 (the proceedings of Crypto '84), published by Springer-Verlag.

CRYPTO 85

A Conference on the Theory and Application of Cryptographic Techniques

held at the University of California, Santa Barbara,
through the co-operation of the
Computer Science Department

August 18-22, 1985

sponsored by

The International Association for Cryptologic Research

in co-operation with

The IEEE Computer Society Technical Committee on Security and Privacy

Organizers

Ernest F. Brickell (Bell Communications Research), General Chairman
H.C. Williams (University of Manitoba), Program Chairman
Thomas A. Berson (Sytek, Inc.), Program
Joan Boyar (University of Chicago), Program
Donald W. Davies (Data Security Consultant), Program
Oded Goldreich (MIT/Technion), Program
Alan G. Konheim (UCSB), Local Arrangements
Carol Patterson (Sandia Laboratories), Registration
Ron Rivest (MIT), Program
Joe Tardo (DEC), Show and Tell

CONTENTS

SECTION I: SIGNATURES AND AUTHENTICATION

SECTION II: PROTOCOLS

SECTION III: COPY PROTECTION

SECTION IV: SINGLE KEY CRYPTOLOGY

SECTION V: TWO KEY CRYPTOLOGY

SECTION VI: RANDOMNESS AND OTHER PROBLEMS

SECTION VII: IMPROMPTU TALKS