Lecture Notes in
Computer Science

Edited by G. Goos and J. Hartmanis

263

A. M. Odlyzko (Ed.)

Advances in Cryptology – CRYPTO '86

Proceedings

Springer-Verlag
Berlin Heidelberg New York London Paris Tokyo

Editor

Andrew M. Odlyzko
AT&T Bell Laboratories
Murray Hill, NJ 07974-2070, USA

CR Subject Classification (1987): E.3

ISBN 3-540-18047-8 Springer-Verlag Berlin Heidelberg New York
ISBN 0-387-18047-8 Springer-Verlag New York Berlin Heidelberg

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

Preface

This book is the proceedings of CRYPTO 86, one in a series of annual conferences devoted to cryptologic research. They have all been held at the University of California at Santa Barbara. The first conference in this series, CRYPTO 81, organized by A. Gersho, did not have a formal proceedings. The proceedings of the following four conferences in this series have been published as:

Advances in Cryptology: Proceedings of Crypto 82, D. Chaum, R. L. Rivest, and A. T. Sherman, eds., Plenum, 1983.

Advances in Cryptology: Proceedings of Crypto 83, D. Chaum, ed., Plenum, 1984.

Advances in Cryptology: Proceedings of CRYPTO 84, G. R. Blakley and D. Chaum, eds., Lecture Notes in Computer Science #196, Springer, 1985.

Advances in Cryptology - CRYPTO '85 Proceedings, H. C. Williams, ed., Lecture Notes in Computer Science #218, Springer, 1986.

A parallel series of conferences is held annually in Europe. The first of these had its proceedings published as

Cryptography: Proceedings, Burg Feuerstein 1982, T. Beth, ed., *Lecture Notes in Computer Science #149*, Springer, 1983.

Eurocrypt 83, held in March of 1983 in Udine, Italy, and Eurocrypt 86, held in May of 1986 in Linköping, Sweden, did not have formal proceedings, while the '84 and '85 conference proceedings have appeared as

Advances in Cryptology: Proceedings of EUROCRYPT 84, T. Beth, N. Cot, and I. Ingemarsson, eds., Lecture Notes in Computer Science #209, Springer, 1985.

Advances in Cryptology - EUROCRYPT '85, F. Pichler, ed., Lecture Notes in Computer Science #219, Springer, 1986.

Papers in this volume are presented in seven sections containing most of the papers presented in the regular program, and a final section based on some of the informal presentations at the "Rump Session" organized by W. Diffie. Several of the regular papers presented at the conference are not included in this volume. There was a special session on integer factorization, and the three papers in that section will be published in journals:

C. Pomerance, J. W. Smith, and R. Tuler, A pipeline architecture for factoring large integers with the quadratic sieve algorithm, SIAM J. Comp. (to appear).

T. R. Caron and R. D. Silverman, Parallel implementation of the quadratic sieve, J. Supercomputing (to appear).

M. C. Wunderlich and H. C. Williams, A parallel version of the continued fraction integer factoring algorithms, J. Supercomputing (to appear).

Also, the paper

J. G. Osborn and J. R. Everhart, A large community key distribution protocol,

was not revised in time for publication.

It is my pleasure to thank all those who make these proceedings possible: the authors, organizers, and all the attendees. Special thanks are due to M. Janssen, Y. Cohen, and the Springer staff for their help in the production of this volume.

Murray Hill, New Jersey Andrew M. Odlyzko

CRYPTO 86

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 11-15, 1986

sponsored by:

The International Association for Cryptologic Research

in co-operation with

*The IEEE Computer Society Technical Committee
on Security and Privacy*

Organizers

General Chairman:	D. Coppersmith (IBM)
Program Committee:	T. A. Berson (Anagram Laboratories)
	E. F. Brickell (Bell Communications Research)
	S. Goldwasser (MIT)
	A. M. Odlyzko (AT&T Bell Laboratories, Chairman)
	C. P. Schnorr (U. Frankfurt)
Local Arrangements:	O. Egelcioglu (UCSB)

TABLE OF CONTENTS

SECTION 1: DATA ENCRYPTION STANDARD

SECTION 2: PUBLIC-KEY CRYPTOGRAPHY

SECTION 3: CRYPTOGRAPHIC PROTOCOLS AND ZERO-KNOWLEDGE PROOFS

SECTION 4: SECRET-SHARING METHODS

SECTION 5: HARDWARE SYSTEMS

SECTION 6: SOFTWARE SYSTEMS

SECTION 7: SOFTWARE PROTECTION, PROBABILISTIC METHODS, AND OTHER TOPICS

SECTION 8: INFORMAL CONTRIBUTIONS