

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

Editorial Board

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

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

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 1987
Printed in Germany

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

| | |
|--|---|
| Structure in the S-boxes of the DES (Extended abstract) | 3 |
| <i>E. F. Brickell, J. H. Moore, and M. R. Puitill</i> | |
| Cycle structure of the DES with weak and semi-weak keys | 9 |
| <i>J. H. Moore and G. J. Simmons</i> | |

SECTION 2: PUBLIC-KEY CRYPTOGRAPHY

| | |
|--|-----|
| Private-key algebraic-coded cryptosystems | 35 |
| <i>T. R. N. Rao and K.-H. Nam</i> | |
| Some variations on RSA signatures and their security | 49 |
| <i>W. de Jonge and D. Chaum</i> | |
| Breaking the Cade cipher | 60 |
| <i>N. S. James, R. Lidl, and H. Niederreiter</i> | |
| A modification of a broken public-key cipher | 64 |
| <i>J. J. Cade</i> | |
| A pseudo-random bit generator based on elliptic logarithms | 84 |
| <i>B. S. Kaliski, Jr.</i> | |
| Two remarks concerning the Goldwasser-Micali-Rivest signature scheme | 104 |
| <i>O. Goldreich</i> | |
| Public-key systems based on the difficulty of tampering (Is there a difference between DES and RSA?) (Extended abstract) | 111 |
| <i>Y. Desmedt and J.-J. Quisquater</i> | |

| | |
|--|-----|
| A secure and privacy-protecting protocol for transmitting personal information between organizations | 118 |
| <i>D. Chaum and J.-H. Evertse</i> | |

SECTION 3: CRYPTOGRAPHIC PROTOCOLS AND ZERO-KNOWLEDGE PROOFS

| | |
|---|-----|
| How to prove all NP-statements in zero-knowledge, and a methodology of cryptographic protocol design (Extended abstract) | 171 |
| <i>O. Goldreich, S. Micali, and A. Wigderson</i> | |
| How to prove yourself: Practical solutions to identification and signature problems | 186 |
| <i>A. Fiat and A. Shamir</i> | |
| Demonstrating that a public predicate can be satisfied without revealing any information about how | 195 |
| <i>D. Chaum</i> | |
| Demonstrating possession of a discrete logarithm without revealing it | 200 |
| <i>D. Chaum, J.-H. Evertse, J. van de Graaf, and R. Peralta</i> | |
| Cryptographic capsules: A disjunctive primitive for interactive protocols | 213 |
| <i>J. Cohen Benaloh</i> | |
| Zero-knowledge simulation of Boolean circuits | 223 |
| <i>G. Brassard and C. Crépeau</i> | |
| All-or-nothing disclosure of secrets | 234 |
| <i>G. Brassard, C. Crépeau, and J.-M. Robert</i> | |
| A zero-knowledge poker protocol that achieves confidentiality of the players' strategy or How to achieve an electronic poker face | 239 |
| <i>C. Crépeau</i> | |

SECTION 4: SECRET-SHARING METHODS

| | |
|--|-----|
| Secret sharing homomorphisms: keeping shares of a secret secret (Extended abstract) | 251 |
| <i>J. Cohen Benaloh</i> | |
| How to share a secret with cheaters | 261 |
| <i>M. Tompa and H. Woll</i> | |
| Smallest possible message expansion in threshold schemes | 266 |
| <i>G. R. Blakley and R. D. Dixon</i> | |

SECTION 5: HARDWARE SYSTEMS

| | |
|---|-----|
| VLSI implementation of public-key encryption algorithms | 277 |
| <i>G. A. Orton, M. P. Roy, P. A. Scott, L. E. Peppard and S. E. Tavares</i> | |
| Architectures for exponentiation in $GF(2^n)$ | 302 |
| <i>T. Beth, B. M. Cook, and D. Gollmann</i> | |
| Implementing the Rivest Shamir and Adleman public key encryption algorithm on a standard digital signal processor | 311 |
| <i>P. Barrett</i> | |

SECTION 6: SOFTWARE SYSTEMS

| | |
|--|-----|
| A high speed manipulation detection code | 327 |
| <i>R. R. Juéneman</i> | |
| Electronic Funds Transfer Point of Sale in Australia | 347 |
| <i>R. Gyoery and J. Seberry</i> | |

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

| | |
|---|-----|
| The notion of security for probabilistic cryptosystems (Extended abstract) | 381 |
| <i>S. Micali, C. Rackoff, and B. Sloan</i> | |
| Large-scale randomization techniques | 393 |
| <i>N. R. Wagner, P. S. Putter, and M. R. Cain</i> | |
| On the linear span of binary sequences obtained from finite geometries | 405 |
| <i>A. H. Chan and R. A. Games</i> | |
| Some constructions and bounds for authentication codes | 418 |
| <i>D. R. Stinson</i> | |
| Towards a theory of software protection (Extended abstract) | 426 |
| <i>O. Goldreich</i> | |

SECTION 8: INFORMAL CONTRIBUTIONS

| | |
|--|-----|
| Two observations on probabilistic primality testing | 443 |
| <i>P. Beauchemin, G. Brassard, C. Crépeau, and C. Goutier</i> | |
| Public-key registration | 451 |
| <i>S. M. Matyas</i> | |
| Is there an ultimate use of cryptography? (Extended abstract) | 459 |
| <i>Y. Desmedt</i> | |
| Smart card, a highly reliable and portable security device | 464 |
| <i>L. C. Guillou and M. Ugon</i> | |

| | |
|--|-----|
| THOMAS - A complete single chip RSA device | 480 |
| <i>G. Rankine</i> | |
| AUTHOR INDEX | 489 |