

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

Editorial Board

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

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

This work is subject to copyright. All rights are reserved, whether the whole or part of the material is concerned, specifically those of translation, reprinting, re-use of illustrations, broadcasting, reproduction by photocopying machine or similar means, and storage in data banks. Under § 54 of the German Copyright Law where copies are made for other than private use, a fee is payable to "Verwertungsgesellschaft Wort", Munich.

© by Springer-Verlag Berlin Heidelberg 1986

Printed in Germany

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 fifth¹ 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
January 1986

H.C.W.

¹Proceedings 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

Breaking the Ong-Schnorr-Shamir Signature Scheme for Quadratic Number Fields	3
<i>Dennis Estes, Leonard M. Adleman, Kireeti Kompella, Kevin S. McCurley, and Gary L. Miller</i>	
Another Birthday Attack	14
<i>Don Coppersmith</i>	
Attacks on Some RSA Signatures	18
<i>Wiebren de Jonge and David Chaum</i>	
An Attack on a Signature Scheme Proposed by Okamoto and Shiraishi	28
<i>Ernest F. Brickell and John M. DeLaurentis</i>	
A Secure Subliminal Channel (?)	33
<i>Gustavus J. Simmons</i>	
Unconditionally Secure Authentication Schemes and Practical and Theoretical Consequences	42
<i>Yvo Desmedt</i>	

SECTION II: PROTOCOLS

On the Security of Ping-Pong Protocols When Implemented Using the RSA	58
<i>Shimon Even, Oded Goldreich, and Adi Shamir</i>	
A Secure Poker Protocol that Minimizes the Effect of Player Coalitions	73
<i>Claude Crepeau</i>	
A Framework for the Study of Cryptographic Protocols	87
<i>Richard Berger, Sampath Kannan, and Rene Peralta</i>	
Cheating at Mental Poker	104
<i>Don Coppersmith</i>	
Security for the DoD Transmission Control Protocol	108
<i>Whitfield Diffie</i>	
Symmetric Public-Key Encryption	128
<i>Zvi Galil, Stuart Haber, and Moti Yung</i>	

SECTION III: COPY PROTECTION

Software Protection: Myth or Reality?	140
<i>James R. Gosler</i>	
Public Protection of Software	158
<i>A. Herzberg and S. Pinter</i>	
Fingerprinting Long Forgiving Messages	180
<i>G.R. Blakley, Catherine Meadows, and G.B. Purdy</i>	

SECTION IV: SINGLE KEY CRYPTOLOGY

Cryptanalysis of DES with a Reduced Number of Rounds	192
<i>David Chaum and Jan-Hendrik Evertse</i>	
Is DES a Pure Cipher? (Results of More Cycling Experiments on DES)	212
<i>Burt S. Kaliski, Ronald L. Rivest, and Alan T. Sherman</i>	
A Layered Approach to the Design of Private Key Cryptosystems	227
<i>T.E. Moore and S.E. Tavares</i>	
Lifetimes of Keys in Cryptographic Key Management Systems	246
<i>E. Okamoto and K. Nakamura</i>	
Correlation Immunity and the Summation Generator	260
<i>Rainer A. Rueppel</i>	
Design of Combiners to Prevent Divide and Conquer Attacks	273
<i>T. Siegenthaler</i>	
On the Security of DES	280
<i>Adi Shamir</i>	
Information Theory Without the Finiteness Assumption, II Unfolding the DES	282
<i>G.R. Blakley</i>	

SECTION V: TWO KEY CRYPTOLOGY

Analysis of a Public Key Approach Based on Polynomial Substitution	340
<i>Harriet Fell and Whitfield Diffie</i>	
Developing an RSA Chip	350
<i>Martin Kochanski</i>	

An M^3 Public-Key Encryption Scheme	358
<i>H.C. Williams</i>	
Trapdoor Rings and Their Use in Cryptography	369
<i>V. Varadharajan</i>	
On Computing Logarithms Over Finite Fields	396
<i>Taher El Gamal</i>	
On Using RSA with Low Exponent in a Public Key Network	403
<i>Johan Hastad</i>	
Lenstra's Factorisation Method Based on Elliptic Curves	409
<i>N.M. Stephens</i>	
Use of Elliptic Curves in Cryptography	417
<i>Victor S. Miller</i>	

SECTION VI: RANDOMNESS AND OTHER PROBLEMS

Cryptography with Cellular Automata	429
<i>Stephen Wolfram</i>	
Efficient Parallel Pseudo-Random Number Generation	433
<i>J.H. Reif and J.D. Tygar</i>	
How to Construct Pseudo-random Permutations from Pseudo-random Functions	447
<i>Michael Luby and Charles Rackoff</i>	
The Bit Security of Modular Squaring Given Partial Factorization of the Modulus	448
<i>Benny Chor, Oded Goldreich, and Shafi Goldwasser</i>	
Some Cryptographic Aspects of Womcodes	458
<i>Philippe Godlewski and Gerard D. Cohen</i>	
How to Reduce Your Enemy's Information	468
<i>Charles H. Bennett, Gilles Brassard, and Jean-Marc Robert</i>	
Encrypting Problem Instances: Or ... Can you Take Advantage of Someone Without Having to Trust Him?	477
<i>Joan Feigenbaum</i>	
Divergence Bounds on Key Equivocation and Error Probability in Cryptanalysis	489
<i>J. van Tilburg and D.E. Boeke</i>	

SECTION VII: IMPROMPTU TALKS

A Chosen Text Attack on the RSA Cryptosystem and Some Discrete Logarithm Schemes	516
<i>Y. Desmedt and A.M. Odlyzko</i>	
On the Design of S-boxes	523
<i>A.F. Webster and S.E. Tavares</i>	
The Real Reason for Rivest's Phenomenon	535
<i>Don Coppersmith</i>	
The Importance of "Good" Key Scheduling Schemes (How to Make a Secure DES Scheme with ≤ 48 Bit Keys?)	537
<i>J.-J. Quisquater, Y. Desmedt, and M. Davio</i>	
Access Control at the Netherlands Postal and Telecommunications Services	543
<i>W. Haemers</i>	
Author Index	545
Keyword Index	546