

Lecture Notes in Computer Science

Edited by G. Goos and J. Hartmanis

293

Carl Pomerance (Ed.)

Advances in Cryptology — CRYPTO '87

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

Carl Pomerance
Department of Mathematics, The University of Georgia
Athens, Georgia 30602, USA

CR Subject Classification (1987): E.3

ISBN 3-540-18796-0 Springer-Verlag Berlin Heidelberg New York

ISBN 0-387-18796-0 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 1988
Printed in Germany

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

Preface

This book is the proceedings of CRYPTO'87, one in a series of annual conferences devoted to cryptologic research. For citations of proceedings of CRYPTO and Eurocrypt conferences before 1986, see

Advances in Cryptology-CRYPTO'86 Proceedings, A. M. Odlyzko, ed.,
Lecture Notes in Computer Science #263, Springer, 1987.

Papers in this volume are organized into seven sections. The first six sections comprise all of the papers on the regular program, including two papers on the program that unfortunately were not presented at the meeting. The seventh section contains some of the papers presented at the "Rump Session" organized by W. Diffie and also includes a short note by T. R. N. Rao which comments on the paper of R. Struik and J. van Tilburg.

CRYPTO'87 was attended by 170 people representing 19 countries. Responsible not only for the conference as a whole, G. B. Agnew also took care of local arrangements in Santa Barbara. We all owe him a debt of gratitude for his highly successful efforts.

It is my special pleasure to thank my fellow members of the Program Committee: T. A. Benson, E. F. Brickell, A. M. Odlyzko, and G. J. Simmons. They all were most prompt, efficient, and willing to cheerfully compromise on disagreements. My task would have been hopeless without them.

I also would like to thank the authors and attendees who made CRYPTO'87 such a success. Special thanks are due to University of Georgia secretaries D. Byrd and P. Sisk and L. B. Montz at Springer for their help in the production of this volume.

Athens, Georgia

Carl Pomerance

CRYPTO'87

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 16-20, 1987

sponsored by:

The International Association for Cryptologic Research

in cooperation with

The IEEE Computer Society Technical Committee
On Security and Privacy

ORGANIZERS

General Chairman: G. B. Agnew (U. Waterloo)

Program Committee: T. A. Berson (Anagram Laboratories)
E. F. Brickell (Bell Communications Research)
A. M. Odlyzko (AT&T Bell Laboratories)
C. Pomerance (U. Georgia, Chairman)
G. J. Simmons (Sandia National Laboratories)

TABLE OF CONTENTS

SECTION 1: COMMUNICATION NETWORKS AND STANDARDS

Standards for data security - a change of direction	3
W. L. Price	
Integrating cryptography in ISDN	9
K. Presttun	

SECTION 2: PROTOCOLS

Special uses and abuses of the Fiat-Shamir passport protocol (Extended abstract)	21
Y. Desmedt, C. Goutier, and S. Bengio	
Direct minimum-knowledge computations (Extended abstract)	40
R. Impagliazzo and M. Yung	
Non-interactive zero-knowledge proof systems	52
A. De Santis, S. Micali, and G. Persiano	
How to solve any protocol problem - an efficiency improvement (Extended abstract)	73
O. Goldreich and R. Vainish	
Multiparty computations ensuring privacy of each party's input and correctness of the result	87
D. Chaum, I. B. Damgård, and J. van de Graaf	
Society and group oriented cryptography: A new concept	120
Y. Desmedt	
A simple and secure way to show the validity of your public key	128
J. van de Graaf and R. Peralta	
Cryptographic computation: Secure fault-tolerant protocols and the public-key model (Extended abstract)	135
Z. Galil, S. Haber, and M. Yung	

Gradual and verifiable release of a secret (Extended abstract)	156
E. F. Brickell, D. Chaum, I. B. Damgård, and J. van de Graaf	
Strong practical protocols	167
J. H. Moore	

SECTION 3: KEY DISTRIBUTION SYSTEMS

Identity-based conference key distribution systems	175
K. Koyama and K. Ohta	
On the key predistribution system: A practical solution to the key distribution problem	185
T. Matsumoto and H. Imai	
Key distribution systems based on identification information	194
E. Okamoto	
Secret distribution of keys for public-key systems (Extended abstract) . .	203
J.-J. Quisquater	

SECTION 4: PUBLIC KEY SYSTEMS

An impersonation-proof identity verification scheme	211
G. J. Simmons	
Arbitration in tamper proof systems (If $DES \approx RSA$ then what's the difference between true signature and arbitrated signature schemes?) . . .	216
G. I. Davida and B. J. Matt	
Efficient digital public-key signatures with shadow (Abstract)	223
L. Guillou and J.-J. Quisquater	
Security-related comments regarding McEliece's public-key cryptosystem	224
C. M. Adams and H. Meijer	

SECTION 5: DESIGN AND ANALYSIS OF CRYPTOGRAPHIC SYSTEMS

Components and cycles of a random function	231
J. M. DeLaurentis	
Fast spectral tests for measuring nonrandomness and the DES	243
F. A. Feldman	
Other cycling tests for DES (Abstract)	255
J.-J. Quisquater and J.-P. Delescaille	

A crypto-engine	257
G. I. Davida and F. B. Dancs	
A natural taxonomy for digital information authentication schemes	269
G. J. Simmons	
Analyzing encryption protocols using formal verification techniques (Extended abstract)	289
R. A. Kemmerer	
Cryptosystems based on an analog of heat flow	306
G. R. Blakley and W. Rundell	
A combinatorial approach to threshold schemes	330
D. R. Stinson and S. A. Vanstone	
A realization scheme for the identity-based cryptosystem	340
H. Tanaka	
Equivalence between two flavours of oblivious transfers	350
C. Crépeau	
A construction for authentication/secretory codes from certain combinatorial designs	355
D. R. Stinson	

SECTION 6: APPLICATIONS

A digital signature based on a conventional encryption function	369
R. C. Merkle	
How to make replicated data secure	379
M. P. Herlihy and J. D. Tygar	
A study of password security	392
M. Luby and C. Rackoff	
A video scrambling technique based on space filling curves (Extended abstract)	398
Y. Matias and A. Shamir	
Secure audio teleconference	418
E. F. Brickell, P. J. Lee, and Y. Yacobi	

SECTION 7: INFORMAL CONTRIBUTIONS

Attack on the Koyama-Ohta identity based key distribution scheme	429
Y. Yacobi	
On the F-function of FEAL	434
W. Fumy	

Patterns of entropy drop of the key in an S-box of the DES (Extended abstract)	438
K. C. Zeng, J. H. Yang, and Z. T. Dai	
The Rao-Nam scheme is insecure against a chosen-plaintext attack	445
R. Struik and J. van Tilburg	
On Struik-Tilburg cryptanalysis of Rao-Nam scheme	458
T. R. N. Rao	
A generalization of Hellman's extension of Shannon's approach to cryptography (Abstract)	461
P. Beauchemin and G. Brassard	
Multiparty unconditionally secure protocols (Abstract)	462
D. Chaum, C. Crépeau, and I. Damgård	
AUTHOR INDEX	463