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.

\(^1\)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

- Breaking the Ong-Schnorr-Shamir Signature Scheme for Quadratic Number Fields ................................. 3  
  *Dennis Estes, Leonard M. Adleman, Kireeti Kompella, Kevin S. McCurley, and Gary L. Miller*

- Another Birthday Attack ............................................................... 14  
  *Don Coppersmith*

- Attacks on Some RSA Signatures ................................................... 18  
  *Wiebren de Jonge and David Chaum*

- An Attack on a Signature Scheme Proposed by Okamoto and Shiraishi ......................................................... 28  
  *Ernest F. Brickell and John M. DeLaurentis*

- A Secure Subliminal Channel (?) .................................................. 33  
  *Gustavus J. Simmons*

- Unconditionally Secure Authentication Schemes and Practical and Theoretical Consequences .............................. 42  
  *Yvo Desmedt*

### SECTION II: PROTOCOLS

- On the Security of Ping-Pong Protocols When Implemented Using the RSA .................................................. 58  
  *Shimon Even, Oded Goldreich, and Adi Shamir*

- A Secure Poker Protocol that Minimizes the Effect of Player Coalitions ................................................... 73  
  *Claude Crepeau*

- A Framework for the Study of Cryptographic Protocols ................................................................. 87  
  *Richard Berger, Sampath Kannan, and Rene Peralta*

- Cheating at Mental Poker ............................................................. 104  
  *Don Coppersmith*

  *Whitfield Diffie*

- Symmetric Public-Key Encryption ................................................ 128  
  *Zvi Galil, Stuart Haber, and Moti Yung*
SECTION III: COPY PROTECTION

Software Protection: Myth or Reality? .................................................... 140
James R. Gosler

Public Protection of Software .............................................................. 158
A. Herzberg and S. Pinter

Fingerprinting Long Forgiving Messages .......................................... 180
G.R. Blakley, Catherine Meadows, and G.B. Purdy

SECTION IV: SINGLE KEY CRYPTOLOGY

Cryptanalysis of DES with a Reduced Number of Rounds .................... 192
David Chaum and Jan-Hendrik Evertse

Is DES a Pure Cipher? (Results of More Cycling Experiments on DES) ........................................................................ 212
Burt S. Kaliski, Ronald L. Rivest, and Alan T. Sherman

A Layered Approach to the Design of Private Key Cryptosystems .......... 227
T.E. Moore and S.E. Tavares

Lifetimes of Keys in Cryptographic Key Management Systems .......... 246
E. Okamoto and K. Nakamura

Correlation Immunity and the Summation Generator .......................... 260
Rainer A. Rueppel

Design of Combiners to Prevent Divide and Conquer Attacks .......... 273
T. Siegenthaler

On the Security of DES ...................................................................... 280
Adi Shamir

Information Theory Without the Finiteness Assumption, II
Unfolding the DES ............................................................................. 282
G.R. Blakley

SECTION V: TWO KEY CRYPTOLOGY

Analysis of a Public Key Approach Based on Polynomial .................... 340
Substitution
Harriet Fell and Whitfield Diffie

Developing an RSA Chip .................................................................... 350
Martin Kochanski
An M³ Public-Key Encryption Scheme ...................................................... 358
    H.C. Williams

Trapdoor Rings and Their Use in Cryptography ........................................... 369
    V. Varadharajan

On Computing Logarithms Over Finite Fields ............................................. 396
    Taher ElGamal

On Using RSA with Low Exponent in a Public Key Network ............................ 403
    Johan Hastad

Lenstra's Factorisation Method Based on Elliptic Curves ............................ 409
    N.M. Stephens

Use of Elliptic Curves in Cryptography ................................................ 417
    Victor S. Miller

SECTION VI: RANDOMNESS AND OTHER PROBLEMS

Cryptography with Cellular Automata .................................................... 429
    Stephen Wolfram

Efficient Parallel Pseudo-Random Number Generation .................................. 433
    J.H. Reif and J.D. Tygar

How to Construct Pseudo-random Permutations from Pseudo-random Functions .... 447
    Michael Luby and Charles Rackoff

The Bit Security of Modular Squaring Given Partial Factorization of the Modulos 448
    Benny Chor, Oded Goldreich, and Shafi Goldwasser

Some Cryptographic Aspects of Womcodes ............................................. 458
    Philippe Godlewski and Gerard D. Cohen

How to Reduce Your Enemy's Information ............................................. 468
    Charles H. Bennett, Gilles Brassard, and Jean-Marc Robert

Encrypting Problem Instances: Or ... Can you Take Advantage of Someone Without Having to Trust Him? 477
    Joan Feigenbaum

Divergence Bounds on Key Equivocation and Error Probability in Cryptanalysis 489
    J. van Tilburg and D.E. Boekee
SECTION VII: IMPROMPTU TALKS

A Chosen Text Attack on the RSA Cryptosystem and Some Discrete Logarithm Schemes ........................................ 516
Y. Desmedt and A.M. Odlyzko

On the Design of S-boxes ............................................................. 523
A.F. Webster and S.E. Tavares

The Real Reason for Rivest's Phenomenon ....................................... 535
Don Coppersmith

The Importance of "Good" Key Scheduling Schemes (How to Make a Secure DES Scheme with ≤ 48 Bit Keys?) .......... 537
J.-J. Quisquater, Y. Desmedt, and M. Davio

Access Control at the Netherlands Postal and Telecommunications Services ..................................................... 543
W. Haemers

Author Index .................................................................................. 545

Keyword Index .............................................................................. 546