

ADVANCES IN CRYPTOGRAPHY

Allen Gersho, Editor

A Report on CRYPTO 81

CRYPTO 81

was sponsored by

The Data and Computer Communications Committees
of the
IEEE Communications Society

with the cooperation of the
Dept. of Electrical and Computer Engineering
University of California, Santa Barbara

The workshop was supported in part by the
National Science Foundation
Award No. ECS81-17145

Organizing Committee

Chairman: Allen Gersho (Univ. Calif., Santa Barbara)

Committee Members:

Leonard Adleman (Univ. Southern Calif.)
Whitfield Diffie (BNR)
Martin Hellman (Stanford)
Richard Kemmerer (Univ. Calif., Santa Barbara)
Alan Konheim (IBM)
Raymond Pickholtz (George Washington Univ.)
Brian Schanning (Mitre)
Gus Simmons (Sandia)
Stephen Weinstein (American Express)

August 18, 1981
Department of Electrical & Computer Engineering
Santa Barbara, California 93106

ADVANCES IN CRYPTOGRAPHY

Allen Gersho, Editor

A Report on CRYPTO 81

ECE Rept No 82-04

CRYPTO 81
The Data and Computer Communications Committee
of the
IEEE Communications Society
with the cooperation of the
Dept. of Electrical and Computer Engineering
University of California, Santa Barbara

IEEE Workshop on Communications Security

held at
National Science Foundation
University of California, Santa Barbara

August 24-26, 1981

Organizing Committee
Chairman: Allen Gersho (Univ. Calif., Santa Barbara)
Committee Members:
Leonard Adleman (Univ. Southern Calif.)
Whitfield Diffie (BNR)
Martin Hellman (Stanford)
Richard Kermener (Univ. Calif., Santa Barbara)
Alan Konheim (IBM)
Raymond Pichholz (George Washington Univ.)
Brian Schneering (Mitre)
Gus Simmons (Sandia)
Stephen Weinstein (American Express)

August 20, 1982
Department of Electrical & Computer Engineering
Santa Barbara, California 93106

Table of Contents

Section A: Theory & Implementation
Ron Rivest, MIT, Chairman

The Generation of Cryptographically Strong
Pseudo-Random Numbers
Adi Shamir, Weizmann Institute (Israel)

On the Necessity of Exhaustive Search
for System-Invariant Cryptanalyses
Martin E. Hellman, Sandia Labs & Stanford University,
Stanford Univ.

Advances in Cryptography

Time-Memory Tradeoffs for
Heidi Adelman & Martin E. Hellman, Stanford Univ.

Preface

This report contains information provided by the authors about the papers presented at CRYPTO 81. In some cases only abstracts were available, in a few cases essentially complete papers have been included, and in most cases an extended abstract or summary is provided. The Table of Contents gives the complete program with the original titles. In a few papers, the authors have provided closely related material with different titles.

This report is more an afterthought than a proceedings. The success of the workshop motivated considerable interest in making available some form of record of the event. The report was prepared for the participants of the workshop and for the use of the National Science Foundation whose support was of tremendous value by providing travel funds for several participants who would not otherwise have been able to attend.

Section B: Applications
Allen Gersho, Editor

A System for Voice-Data or
Data Authentication and Identification
Ron Rivest, Sandia Corp.

One-Way Functions for
Alan Finkelstein, Univ. Calif., Santa Barbara

DES: An Update
Alice Bellare

Some Regular Properties of the DES
Gerald J. Sargis, National Physical Lab (England)

Subtractive Inverters - Alternatives to the DES
Dan E. Morrison, Univ. New Mexico

Table of Contents

Session A: Theory & Implementation Ron Rivest, MIT, Chairman

The Generation of Cryptographically Strong Pseudo-Random Sequences Adi Shamir, Weitzmann Institute (Israel)	1
On the Necessity of Exhaustive Search for System-Invariant Cryptanalysis Martin E. Hellman, Ehud Karnin & Justin Reyneri, Stanford Univ.	2
Time-Memory-Processor Tradeoffs Hamid Amirazizi & Martin E. Hellman, Stanford Univ.	7
Primality Testing Leonard Adleman, USC	10
Coin Flipping by Telephone Manuel Blum, UC Berkeley	11
High-Speed Hardware Implementation of the Knapsack Cipher Paul S. Henry and R. D. Nash, Bell Labs	16
A Polynomial Time Solution for Compact Knapsacks Hamid Amirazizi, Ehud Karnin, & Justin Reyneri, Stanford Univ.	17
Some Comments on the Knapsack Problem Ingemar Ingemarsson, Univ. of Linkoping (Sweden)	20
Variant of a Public Key Cryptosystem based on Goppa codes John P. Jordan, Bell Labs	25

Session B: Algorithms, Techniques, & Funding Ralph Merkle, ELXSI Int'l, Chairman

A System for Point-of-Sale or Access User Authentication and Identification Gus Simmons, Sandia Corp.	31
One-way Sequence for Transaction Verification Alan Konheim, Univ. Calif., Santa Barbara	38
DES '81: An Update Miles Smid, NBS	39
Some Regular Properties of the DES Donald W. Davies, National Physical Lab (England)	41
Subtractive Encryptors - Alternatives to the DES Don R. Morrison, Univ. New Mexico	42

Towards a Design Procedure for Cryptosecure Substitution Boxes J.A. Gordon, Hatfield Polytechnic (England)	53
An Optimally Secure Relativized Cryptosystem Gilles Brassard, Univ. de Montreal	54
Scrambling and Randomization Subhash C. Kak, Louisiana State Univ.	59
A Discussion of NSA Program OCREAE Larry Hatch, NSA	--
<u>Session C Computers, Networks, Key Management</u>	
Steve Kent, BBN, Chairman Tuesday 8:20 a.m.	
MEMO: A Hybrid Approach to Encrypted Electronic Mail Brian P. Scanning, and J. Kowalchuk, Mitre	64
Digital Signature Scheme for Computer Communication Networks H. Meijer and Selim Akl, Queen's Univ.	65
The Design and Analysis of Cryptographic Protocols Richard de Millo, Nancy Lynch, and Michael J. Merritt, Georgia Tech.	71
Local Network Cryptosystem Architecture Thomas Berson, Sytek, Inc.	73
Software Protection Using "Communal Key Cryptosystems" George B. Purdy, Texas A. & M., Gus Simmons, Sandia, and James Studier, Univ. Illinois	79
Some Cryptographic Techniques for File Protection Steven T. Kent, BBN	80
A Password Extension for Improved Human Factors Sig Porter, NCR	81
Key Management from a Security Viewpoint G. Robert Blakley, Texas A. & M.	82
Implementation of a Hybrid RSA/DES Key Management System Y. Alfred Lau and Tom McPnerson, M/A-COM	83
<u>Session D Applications and Issues</u>	
Steve Weinstein, American Express, Chairman	
Cryptography, the Next Two Decades Whitfield Diffie, BNR, Inc.	84
Security Mechanisms in Electronic Cards Stephen B. Weinstein, American Express	109

Current Market: Products, Costs, Trends
 J. Michael Nye, Marketing Consultants Int'l 110

Results on Sampling-based Scrambling for
 Secure Speech Communication 115
 L. Lee and G. Chow, National Taiwan Univ.

Some Thoughts on Speech Encryption 120
 Aaron D. Wyner, Bell Labs

Nonlinear Feedback Shift Register Sequences 121
 H. J. Becker-Racal-Milgo (England)

Evaluating Relative Security of Commercial
 ComSec Devices 124
 Albert L. Lang and Janet T. Vasek,
 Booz, Allen & Hamilton

Limitations on the Use of Encryption to Enforce
 Mandatory Security 130
 Morrie Gasser, Mitre

The Import/Export Dilemma 135
 J. Michael Nye, Marketing Consultants Int'l

Rump Session

Paul S. Henry, Bell Labs, Chairman

Verification by Anonymous Monitors 138
 David Chaum,
 Univ. California, Santa Barbara

Progress in Public Key Cryptography in Great Britain
 Martin Kochanski,
 Telesecurity Ltd.

A General Public Key System 140
 Ernst Henze,
 Univ. Braunschweig (W. Germany)

Discussion of Adleman's Subexponential Algorithm for
 Computing Discrete Logarithms 142
 Tore Herlestam,
 Univ. Lund (Sweden)

Theorem concerning Pseudo-Random Sequences
 Adi Shamir

Protocol for Signing Contracts
Shimon Even,
Technion (Israel)

148

Ill-Formed Thoughts Concerning Oblivious Transfer
Ron Rivest,
MIT

Panel Discussion
National Security and Commercial Security:
Division of Responsibility

154

Whitfield Diffie, BNR (Moderator)
Melville Klein, NSA
Michael L. Dertouzos, MIT
Andrew Gleason, Harvard
Dean Smith. Honeywell

Protocol for Signing Contracts
Shimon Even,
Technion (Israel)

Ill-formed Thoughts Concerning Oblivious Transfer
Ron Rivest,
MIT

Panel Discussion
National Security and Commercial Security:
Division of Responsibility

- Whitfield Diffie, SRR (Moderator)
- Meville Klein, NSA
- Michael L. Dertouzos, MIT
- Andrew Glasson, Harvard
- Dean Smith, Honeywell