ADVANCES IN CRYPTOLOGY

Proceedings of Crypto 82

ADVANCES IN CRYPTOLOGY

Proceedings of Crypto 82

Edited by

DAVID CHAUM

University of California
Santa Barbara, California

RONALD L. RIVEST

and

ALAN T. SHERMAN

Massachusetts Institute of Technology
Cambridge, Massachusetts

SPRINGER SCIENCE+BUSINESS MEDIA, LLC

Library of Congress Cataloging in Publication Data

Workshop on the Theory and Application of Cryptographic Techniques (1982: University of California, Santa Barbara)
Advances in cryptology.

"Proceedings of a Workshop on the Theory and Application of Cryptographic Techniques, held August 23–25, 1982, at the University of California, Santa Barbara, California"—T.p. verso.
Bibliography: p.
Includes indexes.
1. Computers—Access control—Congresses. 2. Cryptography—Congresses. I. Chaum, David. II. Rivest, Ronald L. III. Sherman, Alan T. IV. Title.
QA76.9.A25W67 1982 001.64 83-9492
ISBN 978-1-4757-0604-8 ISBN 978-1-4757-0602-4 (eBook)
DOI 10.1007/978-1-4757-0602-4

Proceedings of a Workshop on the Theory and Application of Cryptographic Techniques, held August 23–25, 1982, at the University of California, Santa Barbara, California

Originally published by Plenum Press, New York in 1983

CRYPTO 82

A Workshop on the Theory and Application of Cryptographic Techniques

held at the University of California, Santa Barbara

August 23–25, 1982

with the cooperation of
the IEEE Communications Society,
the IEEE Information Theory Group,
and the Department of Computer Science
at the University of California, Santa Barbara

Organizers

David Chaum (UCSB), general chairman
Leonard M. Adleman (USC), program committee
Thomas A. Berson (SYTEK), Hatfield conference coordinator
Dorothy Denning (Purdue), program committee
Whitfield Diffie (BNR), program committee
Paul Eggert (UCSB), treasurer
Allen Gersho (UCSB), program committee
John Gordon (Hatfield Polytechnic), organizing committee
David Kahn (Cryptologia), organizing committee
Richard Kemmerer (UCSB), local arrangements chairman
Stephen Kent (BBN), program committee
John Kowalchuk (MITRE), registration
Ronald L. Rivest (MIT), program committee chairman
Alan T. Sherman (MIT), program committee assistant chairman
Stephen Weinstein (AMEX), organizing committee

Preface

In the opening sentence of their seminal 1976 paper, Diffie and Hellman proclaimed: "We stand today on the brink of a revolution in cryptography."[1] Six years later, we find ourselves in the midst of this revolution, surrounded by an explosion of developments in cryptology.

Cryptology is the art of making and breaking codes and ciphers. More generally, cryptology provides techniques for transmitting information in a private, authenticated, and tamper-proof manner. Cryptology was once the exclusive domain of mathematicians, governments, and military forces. But as computer and communications technologies advance, and as we move toward an electronically interconnected society, more and more people now depend on computer mail, electronic business transactions, and computer data banks. Cryptology has become a vital concern of numerous businesses and individuals. Fortunately, the availability of small, fast, and inexpensive computers has made encryption feasible and economical for many applications.

Organized in response to the growing interest in cryptology, CRYPTO 81 was the first major open conference ever devoted to technical cryptologic research.[2] Its successor, CRYPTO 82, was the largest conference of its kind. Held August 23–25, 1982, CRYPTO 82 attracted over 100 participants, including many leading researchers from all over the world. CRYPTO 82 took place at the University of California at Santa Barbara and was held with the cooperation of the IEEE Communications Society, the IEEE Information Theory Group, and the Department of Computer Science at U. C. Santa Barbara.[3] Compiled as the official record of

[1] Whitfield Diffie and Martin E. Hellman, "New Directions in Cryptography," *IEEE Transactions on Information Theory*, IT-22 (November 1976), 644.

[2] Held August 24–26, 1981, CRYPTO 81 took place at the University of California at Santa Barbara. It was sponsored by the IEEE Data and Computer Communications Committees and was supported in part by the National Science Foundation. The CRYPTO 81 proceedings are available as a technical report: Allen Gersho, ed., "Advances in Cryptology: A Report on CRYPTO 81," ECE Report no. 82-04, Department of Electrical and Computer Engineering, U. C. Santa Barbara, Santa Barbara, California 93106.

[3] Additional details about the conference can be found in: David Kahn, "The CRYPTO 82 Conference, Santa Barbara: A Report on a Conference," *Cryptologia*, 7 (January 1983), 1–5.

CRYPTO 82, *Advances in Cryptology: Proceedings of CRYPTO 82* helps to document the current explosion in cryptologic research.

This volume contains 34 papers that were presented at CRYPTO 82, as well as a paper by Donald W. Davies from CRYPTO 81 that did not appear in the CRYPTO 81 proceedings. Most of these papers appear here in print for the first time. As a unique record of the current state of cryptologic research, *Advances in Cryptology: Proceedings of CRYPTO 82* is an invaluable source of information for anyone intrigued by the recent developments in cryptology. *Advances in Cryptology* is also well suited for use as a supplementary textbook in a course in cryptology.

Reflecting the structure of the conference, the proceedings are arranged in six sections. The first five sections contain the main papers of the conference, organized roughly according to the following themes: algorithms and theory, modes of operation, protocols and transaction security, applications, and cryptanalysis. The sixth section contains abstracts describing results presented at the informal "Rump Session."

Each paper in the five main sections was selected by the program committee from brief abstracts submitted in response to a call for papers. The final papers were not formally refereed, and the authors retain full responsibility for the contents of their papers. Several of the papers are preliminary reports of continuing research.

Section I, "Algorithms and Theory," focuses on specific cryptographic algorithms used to encipher messages and on theoretical foundations for the design of secure algorithms. Many of the papers in this section have a number-theoretic flavor.

Section II, "Modes of Operation," explores two major topics: the security of the Data Encryption Standard (DES) and the use of randomization to increase the security of cryptographic algorithms. For example, papers by Donald W. Davies and Robert J. Jueneman investigate the security of DES when used in output feedback mode. The underlying theme of this section is that the security provided by a cryptographic algorithm is determined in part by the way the algorithm is used.

Section III, "Protocols and Transaction Security," studies how protocols can be used to conduct various business transactions electronically. In particular, protocols are discussed for signing checks, making untraceable payments, and enabling two mutually suspicious parties to sign a contract simultaneously. Methods for proving the correctness of such protocols are also examined in detail.

Section IV, "Applications," treats the key management aspects of a number of cryptographic applications, such as protecting personal data cards, controlling access to local networks, and implementing an electronic notary public. This section also includes a paper by Charles Bennett *et al.* suggesting that quantum mechanics, rather than computational complexity, can form the foundation for certain cryptographic schemes.

Section V, "Cryptanalysis," investigates weaknesses of knapsack ciphers. In what is perhaps the most significant unclassified cryptologic paper of the year, Adi Shamir

explains how to break the basic Merkle-Hellman knapsack public-key cryptosystem. Gustavus J. Simmons *et al.* and Leonard M. Adleman describe related discoveries. During the conference, Adleman's presentation was particularly notable for his use of an *Apple II* personal computer to solve an instance of the Graham-Shamir knapsack cipher. Jeff Legarias and Donald W. Davies also presented papers, but these papers were not received in time to be included in the proceedings. Davies's talk, which concluded the session, was a fascinating overview of techniques used by the Allies during WWII to break the *Enigma* cryptograph.

Section VI, "Rump Session," covers a potpourri of cryptologic topics including DES, multi-party protocols, pseudo-random number generators, threshold schemes, randomized stream ciphers, and the RSA nMOS chip. The papers in this section summarize brief impromptu talks given at an informal evening session of the conference.

Unfortunately, a few papers presented at CRYPTO 82 could not be included in this book. A list of these papers appears immediately following the table of contents.

During his opening remarks, David Chaum proposed the formation of an international organization that would further research in cryptology by coordinating and organizing meetings in the area, and by informing its members of relevant events, publications, and work. During CRYPTO 82, attendees nominated a planning committee. The members were Henry J. Beker, Ernest F. Brickell, David Chaum, Whitfield Diffie, Robert R. Jueneman, David Kahn, and Stephen Kent. At the end of the conference, the planning committee held its first meeting, at which it adopted the working title: "The International Association for Cryptologic Research." The committee also laid plans for a meeting in Europe during March 1983 and for a CRYPTO 83 during August 1983.

The editors would like to thank all of the authors, organizers, and other people who made these proceedings possible. We are grateful to Leonard M. Adleman, Dorothy Denning, Whitfield Diffie, and Stephen Kent, who served as session chairmen and members of the program committee. We also thank Allen Gersho for his help on the program committee. Several other people made essential contributions to the conference: John Kowalchuk handled registration; Richard Kemmerer took care of local arrangements; Paul Eggert served as treasurer; and Thomas A. Berson coordinated CRYPTO 82 with the Hatfield conference. We would also like to express our appreciation to John Gordon, David Kahn, and Stephen Weinstein for helping organize the conference. Finally, our thanks go to Inna Sverbilov of MIT and L. S. Marchand of Plenum Press for their patient and cheerful assistance in preparing this book.

Santa Barbara, California D.C.
Cambridge, Massachusetts R.L.R.
January 1983 A.T.S.

Contents

Session II: Modes of Operation
Dorothy Denning, chairperson

Session III: Protocols and Transaction Security
Leonard M. Adleman, chairperson

Session IV: Applications
Stephen Kent, chairperson

Session V: Special Session on Cryptanalysis
Whitfield Diffie, chairperson

The following papers were presented at CRYPTO 82, but were not received in time to be included in this publication:

Session III: Protocols and Transaction Security

Encryption and Protocols
Stephen Kent (Bolt, Beranek, and Newman, Inc.)

Session V: Special Session on Cryptanalysis

The Strongest Knapsack-Based Cryptosystem?
Adi Shamir (Weizmann Institute, Israel)

On Simultaneous Diophantine Approximation Problems
Jeff Lagarias (Bell Laboratories)

The Bombe at Bletchley Park
Donald W. Davies (National Physical Laboratory, England)

Rump Session: Impromptu Talks by Conference Attendees

A Short Report on the Hatfield Conference
John Gordon (Hatfield Polytechnic, England)

What Would You Do if You Got a Secrecy Order?
Pete Olwell (International Phasor Telecom)