Lecture Notes in Computer Science 1294
Edited by G. Goos, J. Hartmanis and J. van Leeuwen

Advisory Board: W. Brauer D. Gries J. Stoer

Burton S. Kaliski Jr. (Ed.)

Advances in Cryptology – CRYPTO '97

17th Annual International
Cryptology Conference
Santa Barbara, California, USA
August 17-21, 1997
Proceedings

Springer

Series Editors

Gerhard Goos, Karlsruhe University, Germany

Juris Hartmanis, Cornell University, NY, USA

Jan van Leeuwen, Utrecht University, The Netherlands

Volume Editor

Burton S. Kaliski Jr.
RSA Laboratories
20 Crosby Drive, Bedford, MA 01730-1402, USA
E-mail: burt@rsa.com

Cataloging-in-Publication data applied for

Die Deutsche Bibliothek - CIP-Einheitsaufnahme

Advances in cryptology : proceedings / CRYPTO '97, 17th Annual International Cryptology Conference, Santa Barbara, California, USA, August 17 - 21, 1997. Burton S. Kaliski (ed.). [IACR]. - Berlin ; Heidelberg ; New York ; Barcelona ; Budapest ; Hong Kong ; London ; Milan ; Paris ; Santa Clara ; Singapore ; Tokyo : Springer, 1997
(Lecture notes in computer science ; Vol. 1294)
ISBN 3-540-63384-7

CR Subject Classification (1991): E.3, G.2.1, D.4.6, K.6.5,F.2.1-2, C.2, J.1, E.4

ISSN 0302-9743
ISBN 3-540-63384-7 Springer-Verlag Berlin Heidelberg New York

Typesetting: Camera-ready by author
SPIN 10546375 06/3142 – 5 4 3 2 1 0 Printed on acid-free paper

Preface

Crypto '97, the Seventeenth Annual Crypto conference organized by the International Association for Cryptologic Research (IACR) in cooperation with the IEEE Computer Society Technical Committee on Security and Privacy and the Computer Science Department of the University of California, Santa Barbara, represents another step forward in the steady progression of the science of cryptology. There is both a tremendous need for and a great amount of work on securing information with cryptologic technology. As one of the two annual meetings held by the IACR, the Crypto conference provides a focal point for presentation and discussion of research on all aspects of this science.

It is thus a privilege to coordinate the efforts of this community in focusing on its steps forward. Crypto '97 is a conference for its community, and to the researchers who have contributed to it — those whose papers appear in the proceedings, those whose submissions were not accepted, and those who have laid the foundation for the work — the community owes a debt of gratitude.

The process of developing a conference program is a challenging one, and this year's committee made the process both enjoyable and effective. My thanks go to Antoon Bosselaers, Gilles Brassard, Johannes Buchmann, Ivan Damgård, Donald Davies, Alfredo de Santis, Susan Langford, James L. Massey, Moni Naor, David Naccache, Tatsuaki Okamoto, Douglas Stinson, Michael J. Wiener, Rebecca Wright, and Yuliang Zheng for many hours of reviewing submissions and presenting their comments to the committee.

My thanks also to the committee's two advisory members, Neal Koblitz and Hugo Krawcyzk, the program chairs of Crypto '96 and '98. Neal's experience from a year ago and Hugo's perspective on the year ahead have helped to make this year's conference what it is, and should provide continuity to the next one.

Continuing a recent tradition, the review process for Crypto '97 was conducted entirely by e-mail and fax, without a program committee meeting. Each submission was assigned anonymously to three committee members (though many submissions were reviewed by more than three people), and decisions were made through several rounds of e-mail discussions. Of the 160 submissions received, the committee accepted 36, of which 35 appear in final form in these proceedings. Except for the papers themselves, nearly all correspondence with authors was also conducted by e-mail.

Gilles Brassard and Oded Goldreich complete this year's program with their invited lectures on quantum information processing and the theoretical foundations of cryptology. My appreciation to both of them, as well as to Stuart Haber, who chairs the conference's informal rump session (whose papers, due to logistics, cannot be included in these proceedings).

The program committee benefited from the expertise of many colleagues: Carlisle Adams, Carlo Blundo, Dan Boneh, Jørgen Brandt, Ran Canetti, Don Coppersmith, Erik De Win, Giovanni Di Crescenzo, Matthew Franklin, Atsushi Fujioka, Eiichiro Fujisaki, Rosario Gennaro, Helena Handschuh, Michael Jacobson Jr., Markus Jakobsson, Joe Kilian, Lars Knudsen, Tetsutaro Kobayashi, Françoise Levy-dit-Vehel, Keith Martin, Markus Maurer, Andreas Meyer, David M'raïhi, Volker Mueller, Stefan Neis, Kobbi Nissim, Kazuo Ohta, Pascal Paillier, Sachar Paulus, Giuseppe Persiano, Erez Petrank, Benny Pinkas, Bart Preneel, Tal Rabin, Omer Reingold, Mike Reiter, Pankaj Rohatgi, Taiichi Saitoh, Berry Schoenmakers, Martin Strauss, Edlyn Teske, Shigenori Uchiyama, Paul Van Oorschot, Susanne Wetzel, and Hugh Williams. My thanks to each one, as well as to any others whom I have inadvertently omitted.

The successful organization of this year's conference is due to its general chair, Bruce Schneier. The functions of general chair and program chair are for the most part independent, but at those times where collaboration was required, Bruce was very helpful, and I appreciate the opportunity to have worked with him. On behalf of Bruce, I would also like to extend my thanks to Raphael Carter and Karen Cooper for their assistance in the organization of Crypto '97.

My work was also not without assistance, and I would like to thank Ari Juels and Gerri Sireen for their participation in administrative aspects of the program.

In the Proverbs, it is written, "It is the glory of God to conceal a thing; but the honour of kings is to search out a matter." The search for knowledge about cryptology — itself the science of secrets — is an essential part of protecting information in today's increasingly open world. Another step in this search is expressed in these proceedings. May the search of such matters, and the search for knowledge about cryptology, continue for many years to come.

Burt Kaliski

June 16, 1997
Bedford, Massachusetts

CRYPTO '97

August 17–21, 1997, Santa Barbara, California, USA

Sponsored by the

International Association for Cryptologic Research (IACR)

in cooperation with

IEEE Computer Society Technical Committee on Security and Privacy
Computer Science Department, University of California, Santa Barbara

General Chair

Bruce Schneier, Counterpane Systems, USA

Program Chair

Burt Kaliski, RSA Laboratories, USA

Program Committee

Antoon Bosselaers ..... Katholieke Universiteit Leuven, Belgium
Gilles Brassard ..... Université de Montréal, Canada
Johannes Buchmann ..... Techniche Hochschule Darmstadt, Germany
Ivan Damgård ..... Aarhus University, Denmark
Donald Davies ..... Royal Holloway College London, United Kingdom
Alfredo de Santis ..... Università di Salerno, Italy
Susan Langford ..... Atalla Corporation, USA
James L. Massey ..... Swiss Federal Institute of Technology, Switzerland
Moni Naor ..... Weizmann Institute, Israel
David Naccache ..... Gemplus, France
Tatsuaki Okamoto ..... NTT Laboratories, Japan
Douglas Stinson ..... University of Nebraska, USA
Michael J. Wiener ..... Entrust Technologies, Canada
Rebecca Wright ..... AT&T Labs, USA
Yuliang Zheng ..... Monash University, Australia

Advisory Members

Neal Koblitz *(Crypto '96 program chair)* ..... University of Washington, USA
Hugo Krawczyk *(Crypto '98 program chair)* IBM T.J. Watson Research Center, USA
..... and Technion, Israel

Contents

Cryptanalysis of Public-Key Cryptosystems (I)

Cryptanalysis of Public-Key Cryptosystems (II)

Information Theory

Invited Lecture

Elliptic Curve Implementation

Number-Theoretic Systems

Distributed Cryptography

Hash Functions

Cryptanalysis of Secret-Key Cryptosystems