Lecture Notes in Computer Science 1462
Edited by G. Goos, J. Hartmanis and J. van Leeuwen

Hugo Krawczyk (Ed.)

Advances in Cryptology – CRYPTO '98

18th Annual International Cryptology Conference
Santa Barbara, California, USA
August 23-27, 1998
Proceedings

Springer

Series Editors

Gerhard Goos, Karlsruhe University, Germany
Juris Hartmanis, Cornell University, NY, USA
Jan van Leeuwen, Utrecht University, The Netherlands

Volume Editor

Hugo Krawczyk
Department of Electrical Engineering Technion
Haifa 32000, Israel
E-mail: hugo@ee.technion.ac.il

Cataloging-in-Publication data applied for

Die Deutsche Bibliothek - CIP-Einheitsaufnahme

Advances in cryptology : proceedings / Crypto '98, 18th Annual International Cryptology Conference, Santa Barbara, California, USA, August 23 - 27, 1998. Hugo Krawczyk (ed.). [IACR]. - Berlin ; Heidelberg ; New York ; Barcelona ; Budapest ; Hong Kong ; London ; Milan ; Paris ; Singapore ; Tokyo : Springer, 1998
(Lecture notes in computer science ; Vol. 1462)
ISBN 3-540-64892-5

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

ISSN 0302-9743
ISBN 3-540-64892-5 Springer-Verlag Berlin Heidelberg New York

Typesetting: Camera-ready by author
SPIN 10638300 06/3142 – 5 4 3 2 1 0 Printed on acid-free paper

Preface

Crypto '98, the Eighteenth Annual Crypto Conference, is sponsored 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, University of California, Santa Barbara (UCSB). The General Chair, Andrew Klapper, is responsible for local organization and registration.

The Program Committee considered 144 papers and selected 33 for presentation. This year's conference program also includes two invited lectures. Michael Rabin will deliver an IACR Distinguished Lecture on the subject of "Authentication". The tradition of IACR Distinguished Lectures at Crypto and Eurocrypt conferences was initiated a few years ago and it honors scientists who have made outstanding contributions to the field of cryptography. Michael Rabin is one of the most prominent pioneers of modern cryptography with many brilliant contributions to the fundamental aspects of this science. The second invited lecture, titled "Cryptography and the Internet", will be delivered by Steve Bellovin. I believe that Bellovin's talk stresses an important point, namely, the need for the active participation of the crypto community in the challenging task of transferring cryptographic science into real-world applications and implementations.

In addition to these two invited lectures, Miles Smid from the US National Institute of Standards and Technology (NIST) will present a first report on the Advanced Encryption Standard (AES) Conference, which takes place shortly before Crypto'98. The AES Conference's goal is to present candidate encryption algorithms from which a new US standard for symmetric encryption is to be produced. Finally, we will have the traditional Rump Session for informal short presentations of new results. Stuart Haber kindly agreed to run this session.

These proceedings include the revised versions of the 33 papers accepted by the Program Committee. These papers were selected from all the submissions to the conference on the basis of perceived originality, quality and relevance to the field of cryptography. Revisions were not checked as to their contents. The authors bear full responsibility for the contents of their papers.

The selection of papers is a difficult and challenging task. I am very grateful to the Program Committee members who did an excellent job in reviewing the submissions in spite of the severe time constraints imposed by the Program Committee's work schedule. Each submission was refereed by at least three reviewers. In total, close to 600 reports were provided by the reviewers – about 18000 lines of text in total! The Program Committee was assisted by a large number of colleagues who reviewed submissions in their areas of expertise. External reviewers included: W. Aiello, A. Antipa, S. Arita, B. Baum-Waidner, D. Beaver, A. Beimel, M. Bellare, J. Benaloh, C. Bennett, C. Berg, J. Black, S. Blake-Wilson, D. Bleichenbacher, G. Bleumer, T. Boogaerts, C. Cachin, J. Camenisch, R. Canetti, B. Chor, S. Contini, R. Cramer, C. Crepeau, G. Di Crescenzo,

J-F. Dhem, U. Feige, M. Fitzi, R. Gallant, J. A. Garay, P. Gemmell, R. Gennaro, J. Giesen, N. Gilboa, O. Goldreich, S. Haber, S. Halevi, T. Helleseth, M. Hirt, R. Impagliazzo, Y. Ishai, G. Itkis, M. Jakobsson, C. Jutla, J. Kilian, F. Koeune, R. Kohlas, T. Krovetz, E. Kushilevtiz, X. Lai, R. Lambert, P. Landrock, A. Lauder, A. Lenstra, P. MacKenzie, D. Malkhi, H. Massias, W. Meier, M. Michels, V. Miller, M. Naor, M. Näslund, K. Nissim, K. Nyberg, H. Peterson, E. Petrank, B. Pinkas, B. Preneel, C. Rackoff, S. Rajagopalan, O. Reingold, P. Rohatgi, A. Rosen, K. Sakurai, P. Shor, R. Sidney, T. Spies, M. Stadler, D. Stinson, Y. Tsiounis, Y. Tsunoo, D. Tygar, S. Ulfberg, R. Venkatesan, M. Waidner, S. Wolf, R. Wright, Y. Yacobi, Y. Yin, A. Young, and O. Ytrehus. My thanks go to all these reviewers and I apologize for any inadvertent omissions. I also wish to thank the committee's two advisory members, Burt Kaliski and Mike Wiener, the program chairs for Crypto '97 and '98, for their advice, help, and support.

Crypto '98 is the first IACR conference with both electronic submissions and an electronic version of the proceedings. The electronic submission option was a clear choice for most authors, with 90% of the papers submitted this way. All credit and thanks for the setup and smooth operation of this process go to Joe Kilian who volunteered to run this first electronic experience for Crypto. To this end, Joe adapted the electronic submission software developed by ACM's SIGACT group. I thank the ACM for allowing the use of their system. The electronic version of these proceedings will be published by Springer and will be available under `http://link.springer.de/series/lncs/`

In organizing the scientific program of the conference and putting together these proceedings I have been assisted by many people in addition to those mentioned above. I would like to especially thank the following people: Tal Rabin for providing me with essential help and support in many of the organizational aspects; Andrew Klapper, the General Chair of the conference, for freeing me from all the issues not directly related to the scientific program and proceedings; Gitta Abraham for secretarial help; Robert Schapire for providing excellent software for automating many of the chores of running a conference program committee; Kevin McCurley for his help with the electronic submissions procedure; Don Coppersmith for much timely help and support.

Finally, I wish to thank the authors of all submissions for making this conference possible, and the authors of accepted papers for their work and cooperation in the production of these proceedings.

June 1998

Hugo Krawczyk
Program Chair
Crypto '98

CRYPTO '98

August 23–27, 1998, 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

Andrew Klapper, University of Kentucky, USA

Program Chair

Hugo Krawczyk, Technion, Israel and IBM Research, USA

Program Committee

Dan Boneh ..... Stanford University, USA
Don Coppersmith ..... IBM Research, USA
Yair Frankel ..... CertCo, USA
Matt Franklin ..... AT&T Labs–Research, USA
Johan Håstad ..... Royal Institute of Technology, Sweden
Lars Knudsen ..... University of Bergen, Norway
Ueli Maurer ..... ETH Zurich, Switzerland
Alfred Menezes ..... Waterloo University, Canada
Andrew Odlyzko ..... AT&T Labs–Research, USA
Rafail Ostrovsky ..... Bellcore, USA
Jean-Jacques Quisquater ..... Université de Louvain, Belgium
Tal Rabin ..... IBM Research, USA
Matt Robshaw ..... RSA Laboratories, USA
Phillip Rogaway ..... University of California at Davis, USA
Rainer Rueppel ..... R^3 Security Engineering AG, Switzerland
Kazue Sako ..... NEC, Japan
Dan Simon ..... Microsoft Research, USA
Moti Yung ..... CertCo, USA

Advisory members

Burt Kaliski (Crypto'97 program chair) ..... RSA Laboratories, USA
Michael J. Wiener (Crypto'99 program chair) ..... Entrust Technologies, Canada

Table of Contents

Block Cipher Design and Analysis

Algebraic Cryptanalysis

Relations Among Cryptographic Primitives

IACR Distinguished Lecture

Algebraic Schemes

Quantum Cryptography

Signatures, Random Functions and Ideal Ciphers

Zero-Knowledge

Implementation

Rights Protection