

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

This work is subject to copyright. All rights are reserved, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, re-use of illustrations, recitation, broadcasting, reproduction on microfilms or in any other way, and storage in data banks. Duplication of this publication or parts thereof is permitted only under the provisions of the German Copyright Law of September 9, 1965, in its current version, and permission for use must always be obtained from Springer - Verlag. Violations are liable for prosecution under the German Copyright Law.

© Springer-Verlag Berlin Heidelberg 1997

Printed in Germany

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 Krawczyk, 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'raihi, 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 Wetzels, 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 Technische 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

Complexity Theory

The Complexity of Computing Hard Core Predicates	1
<i>Mikael Goldmann and Mats Näslund</i>	
Statistical Zero Knowledge Protocols to Prove Modular Polynomial Relations	16
<i>Eiichiro Fujisaki and Tatsuaki Okamoto</i>	
Keeping the SZK-Verifier Honest Unconditionally	31
<i>Giovanni Di Crescenzo, Tatsuaki Okamoto, and Moti Yung</i>	

Invited Lecture

On the Foundations of Modern Cryptography	46
<i>Oded Goldreich</i>	

Cryptographic Primitives

Plug and Play Encryption	75
<i>Donald Beaver</i>	
Deniable Encryption	90
<i>Ran Canetti, Cynthia Dwork, Moni Naor, and Rafail Ostrovsky</i>	

Lattice-Based Cryptography

Eliminating Decryption Errors in the Ajtai-Dwork Cryptosystem	105
<i>Oded Goldreich, Shafi Goldwasser, and Shai Halevi</i>	
Public-Key Cryptosystems from Lattice Reduction Problems	112
<i>Oded Goldreich, Shafi Goldwasser, and Shai Halevi</i>	

Digital Signatures

RSA-Based Undeniable Signatures	132
<i>Rosario Gennaro, Hugo Krawczyk, and Tal Rabin</i>	
Security of Blind Digital Signatures	150
<i>Ari Juels, Michael Luby, and Rafail Ostrovsky</i>	
Digital Signcryption or How to Achieve Cost (Signature & Encryption) \ll Cost (Signature) + Cost (Encryption)	165
<i>Yuliang Zheng</i>	
How to Sign Digital Streams	180
<i>Rosario Gennaro and Pankaj Rohatgi</i>	

Cryptanalysis of Public-Key Cryptosystems (I)

Merkle-Hellman Revisited: A Cryptanalysis of the Qu-Vanstone Cryptosystem Based on Group Factorizations	198
<i>Phong Nguyen and Jacques Stern</i>	
Failure of the McEliece Public-Key Cryptosystem Under Message-Resend and Related-Message Attack	213
<i>Thomas A. Berson</i>	
A Multiplicative Attack Using LLL Algorithm on RSA Signatures with Redundancy	221
<i>Jean-François Misarsky</i>	

Cryptanalysis of Public-Key Cryptosystems (II)

On the Security of the KMOV Public Key Cryptosystem	235
<i>Daniel Bleichenbacher</i>	
A Key Recovery Attack on Discrete Log-Based Schemes Using a Prime Order Subgroup	249
<i>Chae Hoon Lim and Pil Joong Lee</i>	
The Prevalence of Kleptographic Attacks on Discrete-Log Based Cryptosystems	264
<i>Adam Young and Moti Yung</i>	
“Pseudo-Random” Number Generation within Cryptographic Algorithms: The DSS Case	277
<i>Mihir Bellare, Shafi Goldwasser, and Daniele Micciancio</i>	

Information Theory

Unconditional Security Against Memory-Bounded Adversaries	292
<i>Christian Cachin and Ueli Maurer</i>	
Privacy Amplification Secure Against Active Adversaries	307
<i>Ueli Maurer and Stefan Wolf</i>	
Visual Authentication and Identification	322
<i>Moni Naor and Benny Pinkas</i>	

Invited Lecture

Quantum Information Processing: The Good, the Bad and the Ugly	337
<i>Gilles Brassard</i>	

Elliptic Curve Implementation

Efficient Algorithms for Elliptic Curve Cryptosystems	342
<i>Jorge Guajardo and Christof Paar</i>	
An Improved Algorithm for Arithmetic on a Family of Elliptic Curves.....	357
<i>Jerome A. Solinas</i>	

Number-Theoretic Systems

Fast RSA-Type Cryptosystems Using n-adic Expansion	372
<i>Tsuyoshi Takagi</i>	
A One Way Function Based on Ideal Arithmetic in Number Fields.....	385
<i>Johannes Buchmann and Sachar Paulus</i>	

Distributed Cryptography

Efficient Anonymous Multicast and Reception	395
<i>Shlomi Dolev and Rafail Ostrovsky</i>	
Efficient Group Signature Schemes for Large Groups	410
<i>Jan Camenisch and Markus Stadler</i>	
Efficient Generation of Shared RSA Keys.....	425
<i>Dan Boneh and Matthew Franklin</i>	
Proactive RSA	440
<i>Yair Frankel, Peter Gemmell, Philip D. MacKenzie, and Moti Yung</i>	

Hash Functions

Towards Realizing Random Oracles: Hash Functions that Hide All Partial Information.....	455
<i>Ran Canetti</i>	
Collision-Resistant Hashing: Towards Making UOWHFs Practical	470
<i>Mihir Bellare and Phillip Rogaway</i>	
Fast and Secure Hashing Based on Codes.....	485
<i>Lars Knudsen and Bart Preneel</i>	

Cryptanalysis of Secret-Key Cryptosystems

Edit Distance Correlation Attack on the Alternating Step Generator	499
<i>Jovan Dj. Golić and Renato Menicocci</i>	
Differential Fault Analysis of Secret Key Cryptosystems	513
<i>Eli Biham and Adi Shamir</i>	

Cryptanalysis of the Cellular Message Encryption Algorithm	526
<i>David Wagner, Bruce Schneier, and John Kelsey</i>	
Author Index	539
Erratum	540