

Lecture Notes in Computer Science

963

Edited by G. Goos, J. Hartmanis and J. van Leeuwen

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

Springer

Berlin

Heidelberg

New York

Barcelona

Budapest

Hong Kong

London

Milan

Paris

Tokyo

Don Coppersmith (Ed.)

Advances in Cryptology – CRYPTO '95

15th Annual International Cryptology Conference
Santa Barbara, California, USA, August 27-31, 1995
Proceedings



Springer

Series Editors

Gerhard Goos, Universität Karlsruhe, Germany

Juris Hartmanis, Cornell University, NY, USA

Jan van Leeuwen, Utrecht University, The Netherlands

Volume Editor

Don Coppersmith

IBM T.J. Watson Research Center, Mathematical Sciences 32-256

P.O.Box 218, Yorktown Heights, NY 10598, USA

Cataloging-in-Publication data applied for

Die Deutsche Bibliothek - CIP-Einheitsaufnahme

Advances in cryptology : proceedings / CRYPTO '95, 15th Annual International Cryptology Conference, Santa Barbara, California, USA, August 27 - 31, 1995. Don Coppersmith (ed.). - Berlin ; Heidelberg ; New York ; Barcelona ; Budapest ; Hong Kong ; London ; Milan ; Paris ; Tokyo : Springer, 1995 (Lecture notes in computer science ; 963)

ISBN 3-540-60221-6

NE: Coppersmith, Don [Hrsg.]; CRYPTO <15, 1995, Santa Barbara, Calif.>; GT

CR Subject Classification (1991): E.3-4, G.2.1, D.4.6, F2.1-2, C.2, J.1

1991 Mathematics Subject Classification: 94A60, 11T71, 11Yxx, 68P20, 68Q20, 68Q25

ISBN 3-540-60221-6 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 1995

Printed in Germany

Typesetting: Camera-ready by author

SPIN 10486614 06/3142 - 5 4 3 2 1 0 Printed on acid-free paper

PREFACE

The Crypto '95 conference was 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 of the University of California, Santa Barbara. It took place at the University of California, Santa Barbara, from August 27-31, 1995. This was the fifteenth annual Crypto conference; all have been held at UCSB. For the second time, proceedings were available at the conference. The General Chair, Stafford Tavares, was responsible for local organization and registration.

The Program Committee considered 151 papers and selected 36 for presentation. There were also two invited talks. Robert Morris, Sr. gave a talk on "Ways of Losing Information," which included some non-cryptographic means of leaking secrets that are often overlooked by cryptographers. The second talk, "Cryptography - Myths and Realities," was given by Adi Shamir, this year's IACR Distinguished Lecturer. Shamir is the second person to receive this honor, the first having been Gus Simmons at Crypto '94.

These proceedings contain revised versions of the 36 contributed talks. Each paper was sent to at least three members of the program committee for comments. Revisions were not checked on their scientific aspects. Some authors will write final versions of their papers for publication in refereed journals. Of course, the authors bear full responsibility for the contents of their papers.

I am very grateful to the members of the Program Committee for their hard work and the difficult task of selecting one quarter of the submitted papers. Following recent traditions, the submissions were anonymous; and each program committee member could be the author of at most one accepted paper.

We thank the following referees and external experts for their help on various papers: Philippe Béguin, Mihir Bellare, Charles Bennett, Gilles Brassard, Florent Chabaud, Chris Charnes, Yair Frankel, Atsushi Fujioka, Thomas Hardjono, Philippe Hoogvorst, Nobuyuki Imoto, Toshiya Itoh, Sushil Jajodia, Lars Knudsen, Paul Kocher, Mitsuru Matsui, Tsutomu Matsumoto, David M'Raihi, Yi Mu, Rafail Ostrovsky, Eiji Okamoto, Tatsuaki Okamoto, David Pointcheval, Rei Safavi-Naini, Kouichi Sakurai, Jennifer Seberry, Hiroki Shizuya, Dan Simon, Othmar Staffelbach, Jacques Stern, Moti Yung and Xian-Mo Zhang. I apologize for any omissions.

I thank Baruch Schieber and Prabhakar Raghavan for help with software and LaTeX; Barbara White and Peg Cargiulo for secretarial help; and Yvo Desmedt, Jimmy Upton and Peter Landrock for advice on the mechanics.

Finally, thanks go to all who submitted papers for Crypto '95. The success of the conference depends on the quality of its submissions. I am also thankful for all the authors, who cooperated by delivering their final copy to me in a timely fashion for the proceedings.

Don Coppersmith
Program Chair, Crypto '95
IBM Research Division, Yorktown Heights, New York, USA
June, 1995

CRYPTO '95

University of California, Santa Barbara
August 27-31, 1995

Sponsored by the
International Association for Cryptologic Research

in cooperation with the
*IEEE Computer Society Technical Committee
on Security and Privacy*

and the
*Computer Science Department,
University of California, Santa Barbara*

General Chair

Stafford Tavares, Queen's University, Canada

Program Chair

Don Coppersmith, IBM T.J. Watson Research Center, USA

Program Committee

Ross Anderson	Cambridge University, UK
Ernest Brickell	Sandia National Laboratories, USA
Hugo Krawczyk	IBM T.J. Watson Research Center, USA
Susan Langford	Stanford University, USA
Kevin McCurley	Sandia National Laboratories, USA
Willi Meier	HTL Brugg-Windisch, Switzerland
Moni Naor	Weizmann Institute of Science, Israel
Andrew Odlyzko	AT&T Bell Laboratories, USA
Kazuo Ohta	NTT Laboratories, Japan
Josef Pieprzyk	University of Wollongong, Australia
Jean-Jacques Quisquater	UCL-MathRIZK, Belgium
Alan Sherman	Univ. of Maryland Baltimore County, USA
Scott Vanstone	University of Waterloo, Canada
Serge Vaudenay	Ecole Normale Supérieure, France

CONTENTS

MAC and Hash

MD χ -MAC and Building Fast MACs from Hash Functions.....	1
<i>Bart Preneel and Paul C. van Oorschot</i>	
XOR MACs: New Methods for Message Authentication Using Finite Pseudorandom Functions	15
<i>Mihir Bellare, Roch Guérin and Phillip Rogaway</i>	
Bucket Hashing and its Application to Fast Message Authentication.....	29
<i>Phillip Rogaway</i>	

Number Theory I

Fast Key Exchange with Elliptic Curve Systems	43
<i>Richard Schroepel, Hilarie Orman, Sean O'Malley and Oliver Spatscheck</i>	
Fast Server-Aided RSA Signatures Secure Against Active Attacks.....	57
<i>Philippe Béguin and Jean-Jacques Quisquater</i>	
Security and Performance of Server-Aided RSA Computation Protocols.....	70
<i>Chae Hoon Lim and Pil Joong Lee</i>	

Oblivious Transfer

Efficient Commitment Schemes with Bounded Sender and Unbounded Receiver.....	84
<i>Shai Halevi</i>	
Precomputing Oblivious Transfer.....	97
<i>Donald Beaver</i>	
Committed Oblivious Transfer and Private Multi-Party Computation	110
<i>Claude Crépeau, Jeroen van de Graaf and Alain Tapp</i>	
On the Security of the Quantum Oblivious Transfer and Key Distribution Protocols.....	124
<i>Dominic Mayers</i>	

Cryptanalysis I

How to Break Shamir's Asymmetric Basis	136
<i>Thorsten Theobald</i>	
On the Security of the Gollmann Cascades	148
<i>Sang-Joon Park, Sang-Jin Lee and Seung-Cheol Goh</i>	
Improving the Search Algorithm for the Best Linear Expression	157
<i>Kazuo Ohta, Shiho Moriai and Kazumaro Aoki</i>	
On Differential and Linear Cryptanalysis of the RC5 Encryption Algorithm	171
<i>Burton S. Kaliski Jr. and Yiqun Lisa Yin</i>	

Key Escrow

A Simple Method for Generating and Sharing Pseudo-Random Functions, with Applications to Clipper-like Key Escrow Systems	185
<i>Silvio Micali and Ray Sidney</i>	
A Key Escrow System with Warrant Bounds	197
<i>Arjen K. Lenstra, Peter Winkler and Yacov Yacobi</i>	
Fair Cryptosystems, Revisited	208
<i>Joe Kilian and Tom Leighton</i>	
Escrow Encryption Systems Visited: Attacks, Analysis and Designs	222
<i>Yair Frankel and Moti Yung</i>	

Protocols

Robustness Principles for Public Key Protocols	236
<i>Ross Anderson and Roger Needham</i>	

Cryptanalysis II

Cryptanalysis of the Matsumoto and Imai Public Key Scheme of Eurocrypt '88.....	248
<i>Jacques Patarin</i>	
Cryptanalysis Based on 2-Adic Rational Approximation.....	262
<i>Andrew Klapper and Mark Goresky</i>	
A Key-schedule Weakness in SAFER K-64	274
<i>Lars R. Knudsen</i>	
Cryptanalysis of the Immunized LL Public Key Systems	287
<i>Yair Frankel and Moti Yung</i>	

Zero Knowledge, Interactive Protocols

Secure Signature Schemes based on Interactive Protocols.....	297
<i>Ronald Cramer and Ivan Damgård</i>	
Improved Efficient Arguments.....	311
<i>Joe Kilian</i>	
Honest Verifier vs Dishonest Verifier in Public Coin Zero-Knowledge Proofs.....	325
<i>Ivan Damgård, Oded Goldreich, Tatsuaki Okamoto and Avi Wigderson</i>	

Secret Sharing

Proactive Secret Sharing Or: How to Cope With Perpetual Leakage	339
<i>Amir Herzberg, Stanisław Jarecki, Hugo Krawczyk and Moti Yung</i>	
Secret Sharing with Public Reconstruction	353
<i>Amos Beimel and Benny Chor</i>	
On General Perfect Secret Sharing Schemes	367
<i>G. R. Blakley and G. A. Kabatianski</i>	

Number Theory II

NFS with Four Large Primes: An Explosive Experiment	372
<i>Bruce Dodson and Arjen K. Lenstra</i>	
Some Remarks on Lucas-Based Cryptosystems	386
<i>Daniel Bleichenbacher, Wieb Bosma and Arjen K. Lenstra</i>	

Secret Sharing II

Threshold DSS Signatures without a Trusted Party	397
<i>Susan K. Langford</i>	
t -Cheater Identifiable (k,n) Threshold Secret Sharing Schemes	410
<i>Kaoru Kurosawa, Satoshi Obana and Wakaha Ogata</i>	

Everything Else

Quantum Cryptanalysis of Hidden Linear Functions	424
<i>Dan Boneh and Richard J. Lipton</i>	
An Efficient Divisible Electronic Cash Scheme	438
<i>Tatsuaki Okamoto</i>	
Collusion-Secure Fingerprinting for Digital Data	452
<i>Dan Boneh and James Shaw</i>	

Author Index	467
---------------------------	-----