Lecture Notes in Computer Science

Edited by G. Goos and J. Hartmanis

403

S. Goldwasser (Ed.)

Advances in Cryptology – CRYPTO '88

Proceedings

Springer-Verlag
Berlin Heidelberg New York London Paris Tokyo Hong Kong

Editorial Board
D. Barstow W. Brauer P. Brinch Hansen D. Gries D. Luckham
C. Moler A. Pnueli G. Seegmüller J. Stoer N. Wirth

Editor
Shafi Goldwasser
Laboratory for Computer Science, Massachusetts Institute of Technology
545 Technology Square, Cambridge, MA 02139, USA

CR Subject Classification (1987): E.3

ISBN 978-0-387-97196-4 ISBN 978-0-387-34799-8 (eBook)
DOI 10.1007/978-0-387-34799-8

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 other ways, and storage in data banks. Duplication of this publication or parts thereof is only permitted under the provisions of the German Copyright Law of September 9, 1965, in its version of June 24, 1985, and a copyright fee must always be paid. Violations fall under the prosecution act of the German Copyright Law.

© Springer- Verlag Berlin Heidelberg 1990, corrected publication 2019.

2145/3140-543210 – Printed on acid-free paper

Foreword

The papers in this volume were presented at the CRYPTO '88 conference on theory and applications of cryptography, held August 21-25, 1988 in Santa Barbara, California. The conference was sponsored by the International Association for Cryptologic Research (IACR) and hosted by the computer science department at the University of California at Santa Barbara.

The 44 papers presented here comprise: 35 papers selected from 61 extended abstracts submitted in response to the call for papers, 4 invited presentations, and 6 papers selected from a large number of informal rump session presentations.

The papers were chosen by the program committee on the basis of the perceived originality, quality and relevance to the field of cryptography of the extended abstracts submitted. The submissions were not otherwise refereed, and often represent preliminary reports on continuing research.

It is a pleasure to thank many colleagues. Harold Fredricksen singlehandedly made CRYPTO '88 a successful reality. Eric Bach, Paul Barret, Tom Berson, Gilles Brassard, Oded Goldreich, Andrew Odlyzko, Charles Rackoff and Ron Rivest did excellent work on the program committee in putting the technical program together, assisted by kind outside reviewers.

Dawn Crowel at MIT did a super job in publicizing the conference and coordinating the activities of the committee, and Deborah Grupp has been most helpful in the production of this volume. Special thanks are due to Joe Kilian whose humor while assisting me to divide the papers into sessions was indispensable.

Finally, I wish to thank the authors who submitted papers for consideration and the attendants of CRYPTO '88 for their continuing support.

June 1989 Shafi Goldwasser
Cambridge, MA

CRYPTO '88

A Conference on the Theory and Application of Cryptography

held at the University of California, Santa Barbara,
August 21-25, 1988
through the cooperation of the Computer Science Department

Sponsored by:

International Association for Cryptologic Research

in cooperation with

The IEEE Computer Society Technical Committee
On Security and Privacy

General Chair
Harold Fredricksen, Naval Postgraduate School

Program Chair
Shafi Goldwasser, Massachusetts Institute of Technology

Program Committee

Eric Bach	University of Wisconsin
Paul Barret	Computer Security Ltd.
Tom Berson	Anagram Laboratories
Gilles Brassard	University of Montreal
Oded Goldreich	Technion Israel Institute of Technology
Andrew Odlyzko	Bell Laboratories
Charles Rackoff	University of Toronto
Ron Rivest	Massachusetts Institute of Technology

Table of Contents

Session 1: Cryptographic Primitives
Chair: S. Goldwasser

Weakening Security Assumptions and Oblivious Transfer 2
C. Crépeau and J. Kilian (MIT)

Limits on the Provable Consequences of One-Way Permutations (invited talk) 8
R. Impagliazzo (Berkeley) and S. Rudich (U of Toronto)

Generalized Secret Sharing and Monotone Functions 27
J. Benaloh (U of Toronto) and J. Leichter (Yale)

Session 2: Zero-Knowledge
Chair: C. Rackoff

Everything Provable is Provable in Zero-Knowledge 37
M. Ben-Or (Hebrew U.), O. Goldreich (Technion), S. Goldwasser (MIT), J. Håstad (Royal Inst. of Tech), J. Kilian (MIT), S. Micali (MIT) and P. Rogaway (MIT)

A Perfect Zero-Knowledge Proof for a Problem Equivalent to Discrete Logarithm 57
O. Goldreich and E. Kushilevitz (Technion)

Zero-Knowledge with Finite State Verifiers (invited talk) 71
C. Dwork and L. Stockmeyer (IBM)

Session 3: Number Theory
Chair: A. Odlyzko

Intractable Problems in Number Theory (invited talk) 77
E. Bach (U of Wisconsin)

A Family of Jacobians Suitable for Discrete Log Cryptosystems 94
N. Koblitz (U of Washington)

Computation of Approximate L-th Roots Modulo n and Application to Crytography 100
M. Girault, P. Toffin and B. Vallée (U of Caen)

Session 4: Cryptanalysis

Chair: A. Odlyzko

On the McEliece Public-Key Cryptosystem 119
J. van Tilburg (Netherlands)

A Constraint Satisfaction Algorithm for the Automated Decryption of Simple Substitution Ciphers 132
M. Lucks (Southern Methodist U.)

Session 5: Pseudorandomness

Chair: E. Bach

On the Existence of Pseudorandom Generators 146
O. Goldreich (Technion), H. Krawczyk (Technion) and M. Luby (U of Toronto)

On the Randomness of Legendre and Jacobi Sequences 163
I.B. Damgård (Århus U)

Efficient, Perfect Random Number Generators 173
S. Micali (MIT) and C.P. Schnorr (U of Frankfurt)

Session 6: Signatures and Authentication

Chair: E. Bach

How to Sign Given Any Trapdoor Function 200
M. Bellare and S. Micali (MIT)

A "Paradoxical" Indentity-Based Signature Scheme Resulting from Zero-Knowledge 216
L.C. Guillou (CCETT) and J.-J. Quisquater (Philips)

A Modification of the Fiat-Shamir Scheme 232
K. Ohta and T. Okamoto (NTT)

An Improvement of the Fiat-Shamir Identification and Signature Scheme 244
S. Micali (MIT) and A. Shamir (Weizmann Inst)

Session 7: On the Theory of Security I
Chair: R. Rivest

A Basic Theory of Public and Private Cryptosystems (invited talk) .. 249
C. Rackoff (U of Toronto)

Proving Security Against Chosen Cyphertext Attacks 256
M. Blum (Berkeley), P. Feldman (MIT) and S. Micali (MIT)

Non-Interactive Zero-Knowledge with Preprocessing 269
A. De Santis (IBM), S. Micali (MIT) and G. Persiano (Harvard)

Session 8: On the Theory of Security II
Chair: R. Rivest

The Noisy Oracle Problem 284
U. Feige, A. Shamir and M. Tennenholtz (Weizmann Inst)

On Generating Solved Instances of Computational Problems 297
M. Abadi (DEC), E. Allender (Rutgers U), A. Broder (DEC), J. Feigenbaum (Bell) and L.A. Hemachandra (Columbia U)

Bounds and Constructions for Authentication-Secrecy Codes with Splitting 311
M. De Soete (SU of Ghent)

Session 9: Protocols
Chair: G. Brassard

Untraceable Electronic Cash 319
D. Chaum (CMCS), A. Fiat (Tel-Aviv) and M. Naor (IBM)

Payment Systems and Credential Mechanisms with Provable Security Against Abuse by Individuals 328
I.B. Damgård (Århus U)

A Universal Problem in Secure and Verifiable Distributed Computation 336
M.-D. A. Huang and S.-H. Teng (USC)

Session 10: Security Concerns
Chair: G. Brassard

An Abstract Theory of Computer Viruses (invited talk) 354
L.M. Adleman (USC)

Abuses in Cryptography and How to Fight Them 375
Y. Desmedt (Wisconsin)

How to (Really) Share a Secret 390
G.J. Simmons (Sandia)

Session 11: Linear Complexity
Chair: T. Berson

The Strict Avalanche Criterion: Spectral Properties of Boolean Functions and an Extended Definition 450
R. Forré (ETH)

On the Linear Syndrome Method in Cryptoanalysis 469
K. Zeng and M. Huang (USTC)

Aperiodic Linear Complexities of de Bruijn Sequences 479
R.T.C. Kwok and M. Beale (U of Manchester)

Session 12: Systems
Chair: T. Berson

The Application of Smart Cards for RSA Digital Signatures in a Network Comprising both Interactive and Store-and-Forward Facilities 484
J.R. Sherwood and V.A. Gallo (Computer Security Ltd)

Speeding Up Secret Computations with Insecure Auxiliary Devices ... 497
T. Matsumoto, K. Kato and H. Imai (Yokohama NU)

Developing Ethernet Enhanced-Security System 507
B.J. Herbison (DEC)

A Secure Audio Teleconference System 520
D.G. Steer, L. Strawczynski, W. Diffie and M. Wiener (BNR)

SHORT RUMP SESSION PRESENTATIONS
Chair: W. Diffie

Diffie-Hellman is as Strong as Discrete Log for Certain Primes 530
B. den Boer (CMCS)

Secret Error-Correcting Codes (SECC) 540
T. Hwang (Nat. Cheng Kung U.) and T.R.N. Rao (S.W. Lousiana U)

The Detection of Cheaters in Threshold Schemes 564
E.F. Brickell (Sandia) and D.R. Stinson (Manitoba)

On the Power of 1-way Functions 578
S.A. Kurtz (U of Chicago), S.R. Mahaney (Bell) and
J.S. Royer (U of Chicago)

"Practical IP" $\subseteq$ MA 580
G. Brassard (U of Montreal) and I.B. Damgård (Århus U)

Zero-Knowledge Authentication Scheme with Secret Key Exchange .. 583
J. Brandt, I.B. Damgård, P. Landrock, T. Pedersen (Århus U)

Correction to: Advances in Cryptology – CRYPTO '88 .... C1

Author Index 589