BIBLIOTHEQUE DU CERIST

Lecture Notes in Computer Science

Edited by G. Goos and J. Hartmanis

435

G. Brassard (Ed.)

Advances in Cryptology – CRYPTO '89

Proceedings

Springer-Verlag

New York Berlin Heidelberg London Paris Tokyo Hong Kong

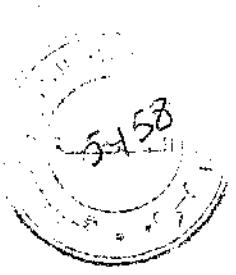
Editorial Board

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

Editor

Gilles Brassard
Département IRO, Université de Montréal
C.P. 6128, Succursale "A"
Montréal (Québec), Canada H3C 3J7

BIBLIOTHEQUE DU CERIST



CR Subject Classification (1987): E.3

ISBN 3-540-97317-6 Springer-Verlag Berlin Heidelberg New York
ISBN 0-387-97317-6 Springer-Verlag New York Berlin Heidelberg

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
Printed in Germany

Printing and binding: Druckhaus Beltz, Hemsbach/Bergstr.
2145/3140-543210 — Printed on acid-free paper

CRYPTO '89

A conference on the Theory and Applications of Cryptology

held at the University of California, Santa Barbara,
through the cooperation of the
Computer Science Department

August 20 – 24, 1989

sponsored by:

The International Association for Cryptologic Research

in cooperation with

The IEEE Computer Society Technical Committee on Security and Privacy

Organizers

General Chairman: Kevin McCURLEY
(IBM Almaden – Sandia National Laboratories

Program Committee:

Josh BENALOH,	University of Toronto
Russell L. BRAND,	Lawrence Livermore Laboratory, Special Session Chairperson
Gilles BRASSARD,	Université de Montréal, Program Committee Chairperson
Claude CRÉPEAU,	Massachusetts Institute of Technology
Whitfield DIFFIE,	Bell Northern Research
Joan FEIGENBAUM,	AT&T Bell Laboratories
James L. MASSEY,	ETH Zentrum, Zurich
Jim OMURA,	Cylink Corporation
Gustavus J. SIMMONS,	Sandia National Laboratories
Scott VANSTONE,	University of Waterloo

BIBLIOTHEQUE DU CERIST

BIBLIOTHEQUE DU CERIST

Preface

Pour Alice
Qui est venue au monde
Trois semaines avant l'avalanche

CRYPTO is a conference devoted to all aspects of cryptologic research. It has been held each year on the campus of the University of California at Santa Barbara since 1981, when it was first organized by Alan Gersho. Annual meetings also take place in Europe under the name of EUROCRYPT. Both CRYPTO and EUROCRYPT conferences are now sponsored by the *International Association for Cryptologic Research* (IACR), which was founded in the wake of CRYPTO '82. You are now holding the proceedings of the ninth CRYPTO meeting: CRYPTO '89. Recent previous proceedings of CRYPTO and EUROCRYPT can be cited as [2, 3, 4, 5, 6]. For citations of yet earlier proceedings, please consult the preface of EUROCRYPT '87 [2].

This year's conference took place on August 20–24, 1989. It attracted 263 participants coming from 23 countries, showing a steady increase in size, and requiring a change to a larger lecture room. This growth is better appreciated if one goes back to the preface of CRYPTO '82, which claims that "[it] was the largest conference of its kind [... it] attracted over 100 participants" [1]! Approximately 40% of the attendees were from the industry, 40% from universities, and 20% from governments. The great success of this year's conference was largely due to the enthusiasm and wonderful work done by Kevin McCurley, who was holding the general chair. We all owe him a debt of gratitude for his total commitment to making CRYPTO '89 a memorable event. For a more elaborate report on CRYPTO '89, please read the report that Kevin has written with my collaboration in the *IACR Newsletter* [8]. Details on the new policies that I enforced as program chairperson can be found in [7].

The call for papers resulted in 93 submissions coming from 18 countries. Out of those, 6 were not considered because they arrived after the deadline, 1 was withdrawn, 45 were accepted, and 2 pairs were asked to merge. The accepted papers were selected by the program committee, sometimes on the basis of a rather short abstract. As an experiment for the CRYPTO conference, I enforced a blind refereeing process by which the name of the authors were not revealed to the other members of the program committee. The final papers were not refereed at all, and the authors retain full responsibility for their contents. Several of the papers are preliminary reports of continuing research. It is anticipated that many of these papers will appear in more polished form in various technical journals, including IACR's *Journal of Cryptology*. There will be a special issue of the *Journal of Cryptology* devoted to some of the best papers of the conference this year. These papers will be refereed by the usual process, and Joan Feigenbaum will serve as the special editor for the issue.

BIBLIOTHEQUE DU CERIST

In addition to the contributed papers, I scheduled three invited talks: "Keying the German navy's Enigma" by David Kahn, "Digital signatures: The evolution of a fundamental primitive" by Silvio Micali, and "A survey of hardware implementations of RSA" by Ernest F. Brickell. Moreover, in order to encourage a balance between practical and theoretical topics at the conferences, this year's program featured an invited special session on practical aspects of cryptology, which was organized and chaired by Russell L. Brand. Thus, 53 regular papers were presented at the conference. Furthermore, 26 additional papers were submitted on the first day of the conference for the traditional "rump session" of impromptu talks organized as always by Whitfield Diffie. Of those, 17 were accepted for short presentation on Tuesday evening, as selected by Whitfield and me.

These proceedings contain papers for all the contributed and all but one of the invited talks given at the conference. The exception is the invited talk of Silvio Micali. Short papers (I imposed a strict limit of four pages) are also included for 8 of the 17 impromptu talks. Reflecting the structure of the conference, the proceedings are arranged in 13 sections (followed by an author index). Each section corresponds to one session of the conference. The first 12 sections contain the contributed and invited papers in the order in which they were presented. The last section is devoted to the rump session. The sections are organized according to the following themes: opening session, why is cryptography harder than it looks?, pseudo-randomness and sequences, cryptanalysis and implementation, signature and authentication I and II, threshold schemes and key management, key distribution and network security, fast computation, odds and ends, zero-knowledge and oblivious transfer, multiparty computation, and the rump session.

Two papers in this collection are of historical significance. The proceedings open with a short paper by David Kahn on the Enigma. You will also find an antique paper by Ralph Merkle, describing "A certified digital signature", which was accepted a decade ago for publication in the *Communications of the ACM*, but which has never seen the light of day. I trust you will agree that despite its old age, this paper has lost none of its interest. Because I wanted Merkle's paper to appear exactly as it was written ten years ago, I allowed the author one page above the otherwise very strict page limit imposed on all other authors. (Please don't throw bricks at me!)

It is my great pleasure to acknowledge the efforts of those who contributed to making the conference and its proceedings possible. First of all, I wish to thank the program committee, without whom my task would have been hopeless. Most of them read and made detailed comments on at least 29 submissions. Besides myself, the committee consisted of Josh Benaloh (University of Toronto), Russell L. Brand (Special session chairperson, Lawrence Livermore National Laboratory), Claude Crépeau (Massachusetts Institute of Technology), Whitfield Diffie (Bell Northern Research), Joan Feigenbaum (AT&T Bell Laboratories), James L. Massey (ETH Zentrum, Zurich), Jim Omura (Cylink Corporation), Gustavus J. Simmons (Sandia National Laboratories), and Scott Vanstone (University of Waterloo). Moreover,

BIBLIOTHEQUE DU CERIST

many colleagues outside the program committee offered their occasional help. Among them, Manuel Blum, Ernest F. Brickell, Jeff Lagarias, Michael Merritt, Larry Ozarow, Carl Pomerance, Jim Reeds, and Moti Yung.

Of course, the most important contribution was that of the authors (including those whose submissions could not be accepted because of the large number of very high quality submissions to the conference this year). I wish to thank the authors for taking so seriously into account my deadline for submission of the final papers. The timeliness of these proceedings is their doing, together with heavy use of electronic mail. More than 300 messages were exchanged by electronic mail between me and the authors, totalizing over half a megabyte of information. Compared to that, I had to make only about 25 long distance phone calls, and 8 FAX's were exchanged.

I also wish to thank the session chairpersons. In addition to program committee members, sessions were chaired by Bob Blakley, Joan Boyar, Ernest F. Brickell, and Kevin McCurley. James L. Massey was scheduled to chair session 10, but he was unfortunately unable to attend the conference because of an accident on the way to the airport. Bob Blakley was kind enough to chair his session on short notice.

Many other people deserve thanks for the organization of the conference. Chief among them, of course, is Kevin McCurley, the general chairperson. I wish to thank also everyone else who took part in the organization of the meeting, IACR officers and directors, and all attendees. I am also grateful to three students who helped me greatly with my task: André Berthiaume, Philippe Hébrais and Sophie Laplante. Lynn Montz and Suzanne Anthony were instrumental at Springer–Verlag in helping me put the proceedings together.

Last but not least, I wish to express my deepest gratitude to my wife Isabelle and newborn daughter Alice for putting up with me while I was working overtime on the program in the spring and on the proceedings in the fall.

Montréal, December 1989 *Gilles Brassard*

BIBLIOTHEQUE DU CERIST

References

[1] *Advances in Cryptology: Proceedings of Crypto 82*, David CHAUM, Ronald L. RIVEST, and Alan L. SHERMAN, Eds., Plenum Press, 1983.

[2] *Advances in Cryptology — EUROCRYPT '87 Proceedings*, David CHAUM and Wyn L. PRICE, Eds., Lecture Notes in Computer Science, Vol. 304, Springer–Verlag, 1988.

[3] *Advances in Cryptology — CRYPTO '87 Proceedings*, Carl POMERANCE, Ed., Lecture Notes in Computer Science, Vol. 293, Springer–Verlag, 1988.

[4] *Advances in Cryptology — EUROCRYPT '88 Proceedings*, Christoph G. GÜNTHER, Ed., Lecture Notes in Computer Science, Vol. 330, Springer–Verlag, 1988.

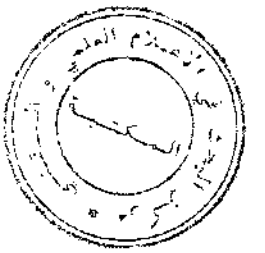
[5] *Advances in Cryptology — CRYPTO '88 Proceedings*, Shafi GOLDWASSER, Ed., Lecture Notes in Computer Science, Springer–Verlag, to appear.

[6] *Advances in Cryptology — EUROCRYPT '89 Proceedings*, Jean–Jacques QUISQUATER, Ed., Lecture Notes in Computer Science, Springer–Verlag, to appear.

[7] BRASSARD, Gilles, "Cryptology — Column 1", *SIGACT News*, Vol. 20, no. 3 (Whole Number 72), pp. 15–19, 1989.

[8] BRASSARD, Gilles and Kevin MCCURLEY, "Crypto '89 conference report", *IACR Newsletter*, Vol. 7, No. 1, pp. 9–11, 1990.

BIBLIOTHEQUE DU CERIST



Contents

Session 1: Opening session

Keying the German navy's Enigma (invited) 2
David KAHN

Making conditionally secure cryptosystems unconditionally abuse-free in a general context 6
Yvo G. DESMEDT

On the existence of bit commitment schemes and zero-knowledge proofs 17
Ivan B. DAMGÅRD

Session 2: Why is cryptography harder than it looks?

Problems with the normal use of cryptography for providing security on unclassified networks (invited) 30
Russell L. BRAND

The use of encryption in Kerberos for network authentication (invited) 35
John T. KOHL

UNIX password security — Ten years later (invited) 44
David C. FELDMEIER and Philip R. KARN

Practical problems with a cryptographic protection scheme (invited) 64
Jonathan M. SMITH

The smart diskette — A universal user token and personal crypto-engine 74
Paul BARRETT and Raymund EISELE

Session 3: Pseudo-randomness and Sequences

On the quadratic spans of periodic sequences 82
Agnes H. CHAN and Richard A. GAMES

The shortest feedback shift register that can generate a given sequence 90
Cees J. A. JANSEN and Dick E. BOEKEE

Perfect local randomness in pseudo-random sequences 100
Ueli M. MAURER and James L. MASSEY

Sparse pseudorandom distributions 113
Oded GOLDREICH and Hugo KRAWCZYK

Bit commitment using pseudo-randomness 128
Moni NAOR

BIBLIOTHEQUE DU CERIST

Session 4: Cryptanalysis and Implementation

How to predict congruential generators 138
Hugo KRAWCZYK

A chosen text attack on the modified cryptographic checksum algorithm of Cohen and Huang 154
Bart PRENEEL, Antoon BOSSELAERS, René GOVAERTS, and Joos VANDEWALLE

On the linear consistency test (LCT) in cryptanalysis with applications 164
Kencheng ZENG, C. H. YANG, and T. R. N. RAO

Batch RSA 175
Amos FIAT

On the implementation of elliptic curve cryptosystems 186
Andreas BENDER and Guy CASTAGNOLI

Session 5: Signature and Authentication I

New paradigms for digital signatures and message authentication based on non-interactive zero knowledge proofs 194
Mihir BELLARE and Shafi GOLDWASSER

Undeniable signatures 212
David CHAUM and Hans VAN ANTWERPEN

Session 6: Signature and Authentication II

A certified digital signature 218
Ralph C. MERKLE

Efficient identification and signatures for smart cards 239
Claus P. SCHNORR

A signature with shared verification scheme 253
Marijke DE SOETE, Jean-Jacques QUISQUATER, and Klaus VEDDER

On-line/off-line digital signatures 263
Shimon EVEN, Oded GOLDREICH, and Silvio MICALI

BIBLIOTHEQUE DU CERIST

Session 7: Threshold schemes and Key management

On the classification of ideal secret sharing schemes 278
Ernest F. BRICKELL and Daniel M. DAVENPORT

Dynamic threshold scheme based on the definition of cross-product in an N-dimensional linear space 286
Chi–Sung LAIH, Lein HARN, Jau–Yien LEE, and Tzonelih HWANG

Secret sharing over infinite domains 299
Benny CHOR and Eyal KUSHILEVITZ

Threshold cryptosystems 307
Yvo G. DESMEDT and Yair FRANKEL

Flexible access control with master keys 316
Gerald C. CHICK and Stafford E. TAVARES

Session 8: Key distribution and Network security

Key distribution protocol for digital mobile communication systems 324
Makoto TATEBAYASHI, Natsume MATSUZAKI, and David B. NEWMAN, JR.

A key exchange system based on real quadratic fields 335
Johannes A. BUCHMANN and Hugh C. WILLIAMS

On key distribution systems 344
Yacov YACOBI and Zahava SHMUELY

SDNS architecture and end-to-end encryption 356
Ruth NELSON and John HEIMANN

Session 9: Fast computation

A survey of hardware implementations of RSA (invited) 368
Ernest F. BRICKELL

Modular exponentiation using recursive sums of residues 371
Paul A. FINDLAY and Brian A. JOHNSON

A fast modular-multiplication algorithm based on a higher radix 387
Hikaru MORITA

Addition chain heuristics 400
Jurjen BOS and Matthijs COSTER

How easy is collision search. New results and applications to DES 408
Jean–Jacques QUISQUATER and Jean–Paul DELESCAILLE

BIBLIOTHEQUE DU CERIST

Session 10: Odds and ends

A Design principle for hash functions 416
Ivan B. DAMGÅRD

One way hash functions and DES 428
Ralph C. MERKLE

Properties of cryptosystem PGM 447
Spyros S. MAGLIVERAS and Nasir D. MEMON

On the construction of block ciphers provably secure and not relying on any unproved hypotheses 461
Yuliang ZHENG, Tsutomu MATSUMOTO, and Hideki IMAI

Disposable zero-knowledge authentications and their applications to untraceable electronic cash 481
Tatsuaki OKAMOTO and Kazuo OHTA

Session 11: Zero-knowledge and Oblivious transfer

Efficient identification schemes using two prover interactive proofs 498
Michael BEN-OR, Shafi GOLDWASSER, Joe KILIAN, and Avi WIGDERSON

On the concrete complexity of zero-knowledge proofs 507
Joan BOYAR and René PERALTA

Zero knowledge proofs of knowledge in two rounds 526
Uriel FEIGE and Adi SHAMIR

Minimum resource zero-knowledge proofs 545
Joe KILIAN, Silvio MICALI, and Rafail OSTROVSKY

Non-interactive oblivious transfer and applications 547
Mihir BELLARE and Silvio MICALI

Session 12: Multiparty computation

Multiparty protocols tolerating half faulty processors 560
Donald BEAVER

Controlled gradual disclosure schemes for random bits and their applications ... 573
Richard CLEVE

Multiparty computation with faulty majority 589
Donald BEAVER and Shafi GOLDWASSER

The Spymasters double-agent problem: Multiparty computations secure unconditionally from minorities and cryptographically from majorities 591
David CHAUM

BIBLIOTHEQUE DU CERIST

Rump session: Impromptu talks

On the structure of secret key exchange protocols 604
Mihir BELLARE, Leonore COWEN, and Shafi GOLDWASSER

An efficient identification scheme based on permuted kernels 606
Adi SHAMIR

An efficient software protection scheme 610
Rafail OSTROVSKY

Good S-boxes are easy to find 612
Carlisle ADAMS and Stafford TAVARES

Covert distributed processing with computer viruses 616
Steve R. WHITE

Progress in data security standardisation 620
Wyn L. PRICE

The FEAL-8 cryptosystem and a call for attack 624
Shoji MIYAGUCHI

How to explain zero-knowledge protocols to your children 628
Jean-Jacques, Myriam, Muriel & Michaël QUISQUATER,
Louis, Marie Annick, Gaïd, Anna, Gwenolé & Soazig GUILLOU,
in collaboration with Tom BERSON for the English version

Author Index 633

BIBLIOTHEQUE DU CERIST