

Lecture Notes in Computer Science

Edited by G. Goos and J. Hartmanis

473

I.B. Damgård (Ed.)

Advances in Cryptology – EUROCRYPT '90

Workshop on the Theory and Application
of Cryptographic Techniques
Aarhus, Denmark, May 21–24, 1990
Proceedings



Springer-Verlag

Berlin Heidelberg New York London
Paris Tokyo Hong Kong Barcelona

Editorial Board

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

Volume Editor

Ivan Bjerre Damgård
Matematisk Institut, Århus Universitet
Ny Munkegade, DK-8000 Århus C, Denmark

CR Subject Classification (1987): D.4.6, E.3, H.2.0

ISBN 3-540-53587-X Springer-Verlag Berlin Heidelberg New York
ISBN 0-387-53587-X 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 current version, and a copyright fee must always be paid. Violations fall under the prosecution act of the German Copyright Law.

© Springer-Verlag Berlin Heidelberg 1991
Printed in Germany

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

Preface

EUROCRYPT is a conference devoted to all aspects of cryptologic research, both theoretical and practical. In the last 7 years, the meeting has taken place once a year at various places in Europe. Both these meetings and the annual Crypto meetings in California are sponsored by The International Association for Cryptologic Research (IACR). Most of the proceedings from these meetings are, like this one, published in Springer-Verlag's *Lecture Notes in Computer Science* series.

EuroCrypt 90 took place on May 21-24 at conference center Scanticon, situated in Århus, Denmark. There were more than 250 participants from all over the world. It is a pleasure to take this opportunity to thank the general chairman Peter Landrock, Århus Congress Bureau, Scanticon, and the organizing committee, who all contributed with hard work and dedication to make a well organized and successful conference.

A total of 85 papers from all over the world were submitted to the conference. This number marks a continuation of the steady growth of interest in the EuroCrypt meetings. Out of the papers submitted, 41 were rejected, 1 was withdrawn, and 2 papers were asked to merge. This resulted in a set of 42 papers presented at the conference. The submissions were in the form of extended abstracts. All program committee members received a full set of submissions, and each submission was refereed independently by at least two members of the program committee (not including the program chairman). The experiment from Crypto 89 with blind refereeing was continued at this conference, and has now become standard policy at IACR conferences. The final papers appearing in these proceedings were not refereed, and the authors retain, of course, full responsibility for the contents. Several of the papers can be expected to appear in various journals in more polished form. There will a special issue of the *Journal of Cryptology* containing selected papers from the conference.

In addition to the formal contributions, a number of informal talks were given at the traditional rump session. These proceedings include short abstracts of some of these impromptu talks.

Finally, it is a pleasure to acknowledge all those who contributed to putting together the program of EuroCrypt 90 and making these proceedings a reality.

First of all, thanks to the program committee. All of its members put a tremendous amount of hard work into the refereeing, and many of them even took the time to make detailed comment on other papers than the 20 they were asked to read carefully. Also some of my colleagues at Århus University kindly offered their help on various technical questions; among these were Torben Pedersen and Jørgen Brandt.

Of course, no conference could have taken place without the authors' contribution. I would like to thank all those who submitted papers, also those whose submissions could not be accepted because of the large number of high quality submissions we received. Many of the authors have been extremely cooperative in changing the format of their papers to fit into the proceedings. Were it not for this attitude, these proceedings would have been significantly delayed.

Århus, September 1990

Ivan Bjerre Damgård

EUROCRYPT 90

A conference on the theory and application of cryptology

Sponsored by The International Association for Cryptologic Research (IACR)

and

CRYPTOMATH_{IC} AS, DATACO AS, Den Danske Bank AS,
Jutland Telephone Company AS

General Chairman: Peter Landrock (Aarhus University)

Organizing Committee:

Jørgen Brandt (Aarhus University)

Palle Brandt Jensen (Jutland Telephone Company)

Torben Pedersen (Aarhus University)

Århus Congress Bureau

Program Chairman: Ivan Damgård (Aarhus University)

Program Committee:

Ueli Maurer (ETH, Zürich)

Andrew J. Clark (Computer Security Ltd., Brighton)

Claude Crépeau (LRI, Paris)

Thomas Siegenthaler (AWK, Zürich)

Joan Boyar (Aarhus University)

Stig Frode Mjølsnes (ELAB, Trondheim)

Marc Girault (SEPT, Caen)

Walter Fumy (Siemens AG, Erlangen)

Othmar Staffelbach (Gretag, Regensburg)

Contents

Session 1: Protocols

<i>All languages in NP have divertible zero-knowledge proofs and arguments under cryptographic assumptions</i> M.V.D. Burmester (University of London) and Y. Desmedt (University of Wisconsin, Milwaukee).....	1
<i>On the importance of memory resources in the security of key exchange protocols</i> G. Davida, Y. Desmedt and R. Peralta (University of Wisconsin, Milwaukee)	11
<i>Provably secure key-updating schemes in identity-based systems,</i> S. Shinozaki, T. Itoh, A. Fujioka and S. Tsujii (Tokyo Institute of Technology).....	16
<i>Oblivious transfer protecting secrecy</i> Bert den Boer (Philips Crypto B.V.).....	31
<i>Public-randomness in public-key cryptography</i> A. De Santis (University of Salerno) and G. Persiano (Harvard University).....	46
<i>An interactive identification scheme based on discrete logarithms and factoring</i> E.F. Brickell and K.S. McCurley (Sandia National Laboratories).....	63

Session 2: Number-Theoretic Algorithms

<i>Factoring with two large primes</i> A.K. Lenstra (Bell Com. Research) and M.S. Manasse (Dig. Equip. Corp.).....	72
<i>Which new RSA signatures can be computed from some given RSA signatures?</i> J.-H. Evertse (University of Leiden) and E. van Heyst (CWI, Amsterdam).....	83
<i>Implementation of a key exchange protocol using real quadratic fields</i> R. Scheidler (University of Manitoba), J.A. Buchman (University of Saarland) and H.C. Williams (University of Manitoba).....	98
<i>Distributed primality proving and the primality of $(2^{3539}+1)/3$</i> F. Morain (INRIA, Le Chesnay).....	110

Session 3: Boolean Functions

<i>Properties of binary functions</i> S. Lloyd (H.P. Laboratories, Bristol).....	124
<i>How to construct pseudorandom permutations from single pseudorandom functions</i> J. Pieprzyk (University of New South Wales).....	140
<i>Constructions of bent functions and difference sets</i> K. Nyberg (University of Helsinki).....	151
<i>Propagation characteristics of boolean functions</i> B. Preneel, W. Van Leekwijk, L. Van Linden, R. Govaerts and J. Vandewalle (K.U. Leuven).....	161

Session 4: Binary Sequences

<i>The linear complexity profile and the jump complexity of keystream sequences</i> H. Niederreiter (Austrian Academy of Sciences).....	174
<i>Lower bounds for the linear complexity of sequences over residue rings</i> Z. Dai (University of Linköping), T. Beth and D. Gollmann (University of Karlsruhe).....	189
<i>On the construction of run permuted sequences</i> C.J.A. Jansen (Philips Crypto B.V.).....	196
<i>Correlation properties of combiners with memory in stream ciphers</i> W. Meier (HTL Brugg-Windisch) and O. Staffelbach (Gretag).....	204
<i>Correlation functions of geometric sequences</i> A.H. Chan, M. Goresky and A. Klapper (Northeastern University).....	214

Session 5: Implementations

<i>Exponentiating faster with addition chains</i> Y. Yacobi (Bellcore).....	222
<i>A cryptographic library for the Motorola DSP 56000</i> S.R. Duse and B.S. Kaliski Jr. (RSA Data Security Inc.).....	230
<i>VICTOR - an efficient RSA hardware implementation</i> H. Orup, E. Svendsen and E. Andreasen (Aarhus University).....	245
<i>Experimental quantum cryptography</i> C.H. Bennett (IBM Yorktown) F. Bessette, G. Brassard, L. Savail (University of Montreal) and J. Smolin (UCLA).....	253

Session 6: Combinatorial Schemes

<i>A protocol to set up shared secret schemes without the assistance of a mutually trusted party</i> I. Ingemarsson (Linköping University) and G. J. Simmons (Sandia Nat. Labs.).....	266
<i>Lower bounds for authentication codes with splitting</i> A. Sgarro (University of Udine).....	283
<i>Essentially 1-fold secure authentication systems</i> A. Beutelspacher (University of Gießen) and U. Rosenbaum (Siemens AG).....	294
<i>On the construction of authentication codes with secrecy and codes withstanding spoofing attacks of order $L \geq 2$</i> B. Smeets, P. Vanrose and Z. Wan (University of Lund).....	306

Session 7: Cryptanalysis

<i>Cryptanalysis of a public-key cryptosystem based on approximations by rational numbers</i>	
J. Stern (University of Paris) and P. Toffin (University of Caen).....	313
<i>A known-plaintext attack on two-key triple encryption</i>	
P.C. van Oorschot and M.J. Wiener (BNR, Ottawa).....	318
<i>Confirmation that some hash functions are not collision free</i>	
S. Miyaguchi, K. Ohta and M. Iwata (NTT Labs).....	326
<i>Inverting the pseudo exponentiation</i>	
F. Bauspieß, H.-J. Knobloch and P. Wichmann (University of Karlsruhe).....	344

Session 8: New Cryptosystems

<i>Cryptosystem for group oriented cryptography</i>	
T. Hwang (Nat. Cheng Kung University).....	352
<i>A provably-secure strongly-randomized cipher</i>	
U. Maurer (Swiss Fed. Inst. of Tech.).....	361
<i>General public key residue cryptosystems and mental poker protocols</i>	
K. Kurosawa, Y. Katayama, W. Ogata and S. Tsujii (Tokyo Inst. of Tech.).....	374
<i>A proposal for a new block encryption standard</i>	
X. Lai and J. Massey (Swiss Fed. Inst. of Tech.).....	389
<i>A new trapdoor in knapsacks</i>	
V. Niemi (University of Turku).....	405

Session 9: Signatures and Authentication

<i>On the design of provably secure cryptographic hash functions</i>	
A. De Santis (University of Salerno) and M. Yung (IBM Yorktown).....	412
<i>Fast signature generation with a Fiat Shamir-like scheme</i>	
H. Ong (Deutsche Bank AG) and C.P. Schnorr (University of Frankfurt).....	432
<i>A remark on a signature scheme where forgery can be proved</i>	
G. Bleumer, B. Pfitzmann and M. Waidner (University of Karlsruhe).....	441
<i>Membership authentication for hierarchical multigroups using the extended Fiat-Shamir scheme</i>	
K. Ohta, T. Okamoto and K. Koyama (NTT Laboratories).....	446
<i>Zero-knowledge undeniable signatures</i>	
D. Chaum (CWI, Amsterdam).....	458
<i>Precautions taken against various potential attacks in ISO/IEC DIS 9796</i>	
L. C. Guillou (CCETT), J.-J. Quisquater (Philips Research), M. Walker (Racal Research), P. Landrock (Aarhus University) and C. Shaer (Racal Research).....	465

Rump Session: Impromptu Talks

<i>Software run-time protection: A cryptographic issue</i> J. Domingo-Ferrer (University of Barcelona).....	474
<i>An identity-based identification scheme based on discrete logarithms modulo a composite number</i> M. Girault (SEPT).....	481
<i>A noisy clock-controlled shift register cryptanalysis concept based on sequence comparison approach</i> J.D. Golic and M.J. Mihaljevic (University of Belgrade).....	487
<i>The MD4 message digest algorithm</i> B.S. Kaliski Jr. (RSA Data Sec. Inc.).....	492
<i>A remark on the efficiency of identification schemes</i> M. Burmester (University of London).....	493
<i>On an implementation of the Mohan-Adiga algorithm</i> Gisela Meister (GAO).....	496