Lecture Notes in Computer Science 1403

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

Kaisa Nyberg (Ed.)

Advances in Cryptology – EUROCRYPT '98

International Conference
on the Theory and Application
of Cryptographic Techniques
Espoo, Finland, May 31 – June 4, 1998
Proceedings

Springer

Series Editors

Gerhard Goos, Karlsruhe University, Germany
Juris Hartmanis, Cornell University, NY, USA
Jan van Leeuwen, Utrecht University, The Netherlands

Volume Editor

Kaisa Nyberg
Finnish Defence Forces, General Staff, CIS Division
Fabianinkatu 2, FIN-00130 Helsinki, Finland
E-mail: Kaisa.Nyberg@mil.fi

Cataloging-in-Publication data applied for

Die Deutsche Bibliothek - CIP-Einheitsaufnahme

Advances in cryptology : proceedings / EUROCRYPT '98,
International Conference on the Theory and Application of
Cryptographic Techniques, Espoo, Finland, May 31 - June 4, 1998.
Kaisa Nyberg (ed.). - Berlin ; Heidelberg ; New York ; Barcelona ;
Budapest ; Hong Kong ; London ; Milan ; Paris ; Santa Clara ;
Singapore ; Tokyo : Springer, 1998
(Lecture notes in computer science ; Vol. 1403)
ISBN 3-540-64518-7

CR Subject Classification (1991): E.3, G.2.1, D.4.6, K.6.5,F.2.1-2, C.2, J.1

ISSN 0302-9743
ISBN 3-540-64518-7 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 1998
Printed in Germany

Typesetting: Camera-ready by author
SPIN 10637126 06/3142 - 5 4 3 2 1 0 Printed on acid-free paper

Preface

The EUROCRYPT '98 conference was organized and sponsored by the International Association for Cryptologic Research in cooperation with and hosted by the Helsinki University of Technology. It took place at the university campus in Espoo, Finland, May 31–June 4, 1998. This year was also the 100th birthday of architect Alvar Aalto, the designer of the Main Hall of the University of Technology where the presentations the 17th annual EUROCRYPT conference were held. Professor Arto Karila, the General Chair, was responsible for local organization. His contribution to the success of the conference is gratefully acknowledged. I would also like to thank Tuomas Aura for managing practical arrangements and creating and maintaining the conference website.

The scientific program for EUROCRYPT '98 was put together by an 18-member program committee which considered 161 submissions by researchers from all over the world. The quality of the submissions was exceptionally high, as is reflected in the number of contributions published in these proceedings, which contain the revised versions of 44 papers accepted for presentation. Still, many good papers had to be left out.

I would like to thank the members of the program committee who devoted an enormous amount of time and energy to reading the papers and making the difficult selection. In addition, I gratefully acknowledge the support to the program commitee by the following experts: Klaus Becker, Simon Blackburn, Daniel Bleichenbacher, Antoon Bosselaers, Karl Brincat, Mike Burmester, Claude Carlet, Cunsheng Ding, DengGuo Feng, Steven Galbraith, Mika Hirvensalo, Shao-Quan Jiang, Juhani Karhumäki, Lars Knudsen, Kaoru Kurosawa, Keith Martin, Alexandru Mateescu, Willi Meier, Tommi Meskanen, Chris Mitchell, Thomas Mittelholzer, Sean Murphy, Phong Nguyen, Kazuo Ohta, Eiji Okamoto, Tatsuaki Okamoto, René Peralta, Holger Petersen, Andreas Pfitzmann, Josef Pieprzyk, Thomas Pornin, Guillaume Poupard, Ari Renvall, Vincent Rijmen, Ahmad-Reza Sadeghi, Kazue Sako, Ruediger Schack, Matthias Schunter, Jacques Stern, Douglas Stinson, Keisuke Tanaka, Michael Waidner, Uta Wille, Qibin Zhai, Xianmo Zhang, Junhui Yang, DingFeng Ye, and Øyvind Ytrehus.

Finally, I would like to thank all authors who submitted papers to EUROCRYPT '98 and, in particular, the authors of the accepted papers for their cooperation in producing these proceedings.

March 1998 Kaisa Nyberg

Eurocrypt '98

May 31–June 4, 1998, Espoo, Finland

Sponsored by the
International Association for Cryptologic Research (IACR)

General Chair

Arto Karila, Helsinki University of Technology, Finland

Program Chair

Kaisa Nyberg, Finnish Defence Forces, Finland

Program Committee

Zongduo Dai	Academia Sinica, China
Yvo Desmedt	University of Wisconsin, USA
Hans Dobbertin	BSI, Germany
Dieter Gollman	Microsoft, U.K.
Tor Helleseth	University of Bergen, Norway
Markus Jakobsson	Bell Labs, USA
Thomas Johansson	University of Lund, Sweden
Xueija Lai	R3 Security Engineering AG, Switzerland
Arjen K. Lenstra	Citibank, USA
Mitsuru Matsui	Mitsubishi, Japan
Torben Pedersen	Cryptomathic, Denmark
Birgit Pfitzmann	University of Saarland, Germany
Bart Preneel	K.U.Leuven, Belgium
Rei Safavi-Naini	University of Wollongong, Australia
Arto Salomaa	University of Turku, Finland
Othmar Staffelbach	UG FU, Switzerland
Serge Vaudenay	Ecole Normale Supérieure, France
Moti Yung	CertCo, USA

CONTENTS

Distributed Cryptography and Applications I

Securing threshold cryptosystems against chosen ciphertext attack 1
Victor Shoup and Rosario Gennaro

Auto-recoverable auto-certifiable cryptosystems 17
Adam Young and Moti Yung

A practical and provably secure scheme for publicly verifiable secret sharing and its applications 32
Eiichiro Fujisaki and Tatsuaki Okamoto

Complexity Theory: Reductions and Lower Bounds

Equivalence of counting the number of points on elliptic curve over the ring $\mathbb{Z}_n$ and factoring n 47
Noboru Kunihiro and Kenji Koyama

Breaking RSA may not be equivalent to factoring 59
Dan Boneh and Ramarathnam Venkatesan

Lower bounds on generic algorithms in groups 72
Ueli Maurer and Stefan Wolf

Cryptanalysis of Block Ciphers

Improved cryptanalysis of RC5 85
Alex Biryukov and Eyal Kushilevitz

Cryptanalysis of the ANSI X9.52 CBCM mode 100
Eli Biham and Lars R. Knudsen

Differential-linear weak key classes of IDEA 112
Philip Hawkes

Distributed Cryptography and Applications II

Divertible protocols and atomic proxy cryptography 127
Matt Blaze, Gerrit Bleumer, and Martin Strauss

Optimum traitor tracing and asymmetric schemes 145
Kaoru Kurosawa and Yvo Desmedt

Computational Algorithms

On finding small solutions of modular multivariate polynomial equations 158
Charanjit S. Jutla

Computing discrete logarithms with quadratic number rings 171
Damian Weber

Improved algorithms for isomorphisms of polynomials 184
Jacques Patarin, Louis Goubin and Nicolas Courtois

Improving Computational Efficiency

Visual cryptanalysis 201
Adi Shamir

How to improve an exponentiation black-box 211
Gérard Cohen, Antoine Lobstein, David Naccache, and Gilles Zémor

Speeding up discrete log and factoring based schemes via precomputations 221
Victor Boyko, Marcus Peinado, and Ramarathnam Venkatesan

Fast batch verification for modular exponentiation and digital signatures . . 236
Mihir Bellare, Juan A. Garay, and Tal Rabin

Paradigms for Symmetric Systems

A formal treatment of remotely keyed encryption 251
Matt Blaze, Joan Feigenbaum, and Moni Naor

Luby-Rackoff backwards: Increasing security by making block ciphers non-invertible 266
Mihir Bellare, Ted Krovetz, and Phillip Rogaway

The chain & sum primitive and its applications to MACs and stream ciphers 281
Mariusz H. Jakubowski and Ramarathnam Venkatesan

Public Key Cryptosystems

A cryptosystem based on non-maximal imaginary quadratic orders with fast decryption 294
Detlef Hühnlein, Michael J. Jacobson, Sachar Paulus, and Tsuyoshi Takagi

A new public-key cryptosystem as secure as factoring 308
Tatsuaki Okamoto and Shigenori Uchiyama

Complexity Theory: One-Way Functions

Towards a better understanding of one-wayness:
Facing linear permutations 319
Alain P. Hiltgen

Finding collisions on a one-way street:
Can secure hash functions be based on general assumptions? 334
Daniel R. Simon

Multi-party Computation

Secure communication in minimal connectivity models 346
Matthew Franklin and Rebecca N. Wright

On the foundations of oblivious transfer 361
Christian Cachin

Quorum-based secure multi-party computation 375
Donald Beaver and Avishai Wool

Digital Signatures

Strengthened security for blind signatures 391
David Pointcheval

Generic constructions for secure and efficient
confirmer signature schemes 406
Markus Michels and Markus Stadler

Security analysis of a practical "on the fly" authentication
and signature generation 422
Guillaume Poupard and Jacques Stern

Untraceability in Multi-party Schemes

Universally verifiable mix-net with verification work independent
of the number of mix-servers 437
Masayuki Abe

A practical mix 448
Markus Jakobsson

Boolean Functions

On the propagation criterion of degree ℓ and order k 462
Claude Carlet

Highly nonlinear balanced Boolean functions
with a good correlation-immunity 475
Eric Filiol and Caroline Fontaine

Heuristic design of cryptographically strong balanced Boolean functions . . . 489
William Millan, Andrew Clark, and Ed Dawson

Combinatorial Design and Analysis of Distributed Schemes

Secret sharing schemes with bipartite access structure 500
Carles Padró and Germán Sáez

Combinatorial bounds for broadcast encryption 512
Michael Luby and Jessica Staddon

New results on multi-receiver authentication codes 527
Rei Safavi-Naini and Huaxiong Wang

Cryptanalysis of Elliptic Curve Systems

Specialized integer factorization 542
Don Coppersmith

Security of an identity-based cryptosystem and the related reductions 546
Tatsuaki Okamoto and Shigenori Uchiyama

Electronic Commerce and Payment

Easy come - easy go divisible cash 561
Agnes Chan, Yair Frankel, and Yiannis Tsiounis

Secure and efficient metering 576
Moni Naor and Benny Pinkas

Optimistic fair exchange of digital signatures 591
N. Asokan, Victor Shoup, and Michael Waidner

Author Index 607