Lecture Notes in Computer Science 2332
Edited by G. Goos, J. Hartmanis, and J. van Leeuwen

Springer
Berlin
Heidelberg
New York
Barcelona
Hong Kong
London
Milan
Paris
Tokyo

Lars Knudsen (Ed.)

Advances in Cryptology – EUROCRYPT 2002

International Conference on the Theory
and Applications of Cryptographic Techniques
Amsterdam, The Netherlands, April 28 – May 2, 2002
Proceedings

Springer

Volume Editor

Lars R. Knudsen
Technical University of Denmark, Department of Mathematics
Building 303, 2800 Lyngby, Denmark
E-mail: knudsen@mat.dtu.dk

Cataloging-in-Publication Data applied for

Die Deutsche Bibliothek - CIP-Einheitsaufnahme

Advances in cryptology : proceedings / EUROCRYPT 2002, International Conference on the Theory and Application of Cryptographic Techniques, Amsterdam, The Netherlands, April 28 - May 2, 2002. Lars Knudsen (ed.). - Berlin ; Heidelberg ; New York ; Barcelona ; Hong Kong ; London ; Milan ; Paris ; Tokyo : Springer, 2002
(Lecture notes in computer science ; Vol. 2332)
ISBN 3-540-43553-0

CR Subject Classification (1998): E.3, G.2.1, D.4.6, K.6.5, F.2.1-2, C.2, J.1

ISSN 0302-9743
ISBN 3-540-43553-0 Springer-Verlag Berlin Heidelberg New York

Springer-Verlag Berlin Heidelberg New York
a member of BertelsmannSpringer Science+Business Media GmbH

http://www.springer.de

Typesetting: Camera-ready by author, data conversion by Steingräber Satztechnik GmbH, Heidelberg
Printed on acid-free paper SPIN: 10869749 06/3142 5 4 3 2 1 0

Preface

You are reading the proceedings of EUROCRYPT 2002, the 21st annual Eurocrypt conference. The conference was sponsored by the IACR, the International Association of Cryptologic Research, `www.iacr.org`, this year in cooperation with the Coding and Crypto group at the Technical University of Eindhoven in The Netherlands. The General Chair, Berry Schoenmakers, was responsible for the local organization, and the conference registration was handled by the IACR Secretariat at the University of California, Santa Barbara, USA. I thank Berry Schoenmakers for all his work and for the pleasant collaboration.

A total of 122 papers were submitted of which 33 were accepted for presentation at the conference. One of the papers is a result of a merger of two submissions. Three additional submissions were withdrawn by the authors shortly after the submission deadline. The program also lists invited talks by Joan Daemen and Vincent Rijmen ("AES and the Wide Trail Strategy") and Stephen Kent ("Rethinking PKI: What's Trust Got To Do with It?"). Also, there was a rump (recent results) session, which Henk van Tilborg kindly agreed to chair.

The reviewing process was a challenging task and many good submissions had to be rejected. Each paper was reviewed by at least three members of the program committee, and papers co-authored by a member of the committee were reviewed by at least five other members. In most cases extensive comments were passed on to the authors. It was a pleasure for me to work with the program committee, whose members all worked very hard over several months. The reviewing process was finalized with a meeting in Copenhagen, on January 13th, 2002.

I am very grateful to the many additional reviewers who contributed with their expertise: Adam Back, Alfred Menezes, Alice Silverberg, Anton Stiglic, Antoon Bosselaers, Ari Juels, Barry Trager, Carlo Blundo, Chan Sup Park, Chong Hee Kim, Christian Paquin, Christophe De Cannière, Craig Gentry, Dae Hyun Yum, Dan Bernstein, Dario Catalano, David Pointcheval, David Wagner, Dong Jin Park, Dorian Goldfeld, Eliane Jaulmes, Emmanuel Bresson, Florian Hess, Frederik Vercauteren, Frédéric Légaré, Frédéric Valette, Glenn Durfee, Guillaume Poupard, Gwenaelle Martinet, Han Pil Kim, Hein Roehrig, Hovav Shacham, Ilya Mironov, Jacques Stern, Jae Eun Kang, Jan Camenisch, Jean-Francois Raymond, Jens Jensen, Jesper Buus Nielsen, Jim Hughes, John Malone-Lee, Jonathan Poritz, Jong Hoon Shin, Katsuyuki Takashima, Kazue Sako, Kenny Paterson, Kyung Weon Kim, Leo Reyzin, Louis Granboulan, Louis Salvail, Markku-Juhani O. Saarinen, Matt Robshaw, Michael Quisquater, Michael Waidner, Michel Mitton, Mike Szydlo, Mike Wiener, Moti Yung, Olivier Baudron, Omer Reingold, Paul Dumais, Paul Kocher, Philippe Chose, Philippe Golle, Pierre-Alain Fouque, Ran Canetti, Richard Jozsa, Ronald Cramer, Sang Gyoo Sim, Sang Jin Lee, Serge Fehr, Shirish Altekar, Simon Blackburn, Stefan Wolf, Steven Galbraith, Svetla Nikova, Tae Gu Kim, Tal Malkin, Tal Rabin, Tetsu Iwata, Toshio Hasegawa, Tsuyoshi Nishioka, Virgil Gligor, Wenbo Mao, Yeon Kyu Park, Yiqun Lisa Yin, Yong Ho Hwang, Yuval Ishai.

My work as program chair was made a lot easier by the electronic submission software written by Chanathip Namprempre for Crypto 2000 with modifications by Andre Adelsbach for Eurocrypt 2001, and by the reviewing software developed and written by Bart Preneel, Wim Moreau, and Joris Claessens for Eurocrypt 2000. I would like to thank Ole da Silva Smith for setting up all this software locally and for the help with the problems I encountered. I am also grateful to Wim Moreau and Chanathip Namprempre for solving some of the problems we had with the software.

On behalf of the general chair I would like to extend my gratitude to the members of the local organizing committee at TU Eindhoven, in particular to Peter Roelse and Gergely Alpár. For financial support of the conference the organizing committee gratefully acknowledges this year's sponsors: Philips Semiconductors Cryptology Competence Center, Mitsubishi Electric Corporation, cv cryptovision, Cryptomathic, ERCIM, CMG, Sectra, EUFORCE, and EIDMA.

Finally, a thank-you goes to all who submitted papers to this conference and last but not least to my family for their love and understanding.

February 2002 Lars Knudsen

EUROCRYPT 2002

April 28–May 2, 2002, Amsterdam, The Netherlands

Sponsored by the

International Association of Cryptologic Research (IACR)

in cooperation with

The Coding and Crypto group at the Technical University of Eindhoven in The Netherlands

General Chair

Berry Schoenmakers, Department of Mathematics and Computing Science, Technical University of Eindhoven, The Netherlands

Program Chair

Lars R. Knudsen, Department of Mathematics, Technical University of Denmark

Program Committee

Dan Boneh ..... Stanford University, USA
Stefan Brands ..... McGill University School of Computer Science, Montreal, Canada
Christian Cachin ..... IBM Research, Zurich, Switzerland
Don Coppersmith ..... IBM Research, USA
Ivan Damgård ..... Aarhus University, Denmark
Anand Desai ..... NTT Multimedia Communications Laboratories, USA
Rosario Gennaro ..... IBM Research, USA
Alain Hiltgen ..... UBS, Switzerland
Markus Jakobsson ..... RSA Laboratories, USA
Thomas Johansson ..... University of Lund, Sweden
Antoine Joux ..... DCSSI, France
Pil Joong Lee ..... Postech, Korea
Arjen Lenstra ..... Citibank and Technical University of Eindhoven
Keith Martin ..... Royal Holloway, University of London, UK
Mitsuru Matsui ..... Mitsubishi Electric, Japan
Phong Q. Nguyen ..... CNRS/Ecole Normale Supérieure, France
Kaisa Nyberg ..... Nokia Research Center, Finland
Bart Preneel ..... Katholieke Universiteit Leuven, Belgium
Reihaneh Safavi-Naini ..... University of Wollongong, Australia
Nigel Smart ..... University of Bristol, UK
Paul Van Oorschot ..... Carleton University, Canada
Rebecca Wright ..... DIMACS, USA

Table of Contents

Cryptanalysis I

Cryptanalysis of a Pseudorandom Generator Based on Braid Groups 1
Rosario Gennaro, Daniele Micciancio

Potential Weaknesses of the Commutator Key Agreement Protocol Based on Braid Groups 14
Sang Jin Lee, Eonkyung Lee

Extending the GHS Weil Descent Attack 29
Steven D. Galbraith, Florian Hess, Nigel P. Smart

Public-Key Encryption

Universal Hash Proofs and a Paradigm for Adaptive Chosen Ciphertext Secure Public-Key Encryption 45
Ronald Cramer, Victor Shoup

Key-Insulated Public Key Cryptosystems 65
Yevgeniy Dodis, Jonathan Katz, Shouhuai Xu, Moti Yung

On the Security of Joint Signature and Encryption 83
Jee Hea An, Yevgeniy Dodis, Tal Rabin

Invited Talk

AES and the Wide Trail Design Strategy 108
Joan Daemen, Vincent Rijmen

Information Theory & New Models

Indistinguishability of Random Systems 110
Ueli Maurer

How to Fool an Unbounded Adversary with a Short Key 133
Alexander Russell, Hong Wang

Cryptography in an Unbounded Computational Model 149
David P. Woodruff, Marten van Dijk

Implementational Analysis

Performance Analysis and Parallel Implementation of Dedicated Hash Functions 165
Junko Nakajima, Mitsuru Matsui

Fault Injection and a Timing Channel on an Analysis Technique 181
John A. Clark, Jeremy L. Jacob

Speeding Up Point Multiplication on Hyperelliptic Curves with Efficiently-Computable Endomorphisms 197
Young-Ho Park, Sangtae Jeong, Jongin Lim

Stream Ciphers

Fast Correlation Attacks: An Algorithmic Point of View 209
Philippe Chose, Antoine Joux, Michel Mitton

BDD-Based Cryptanalysis of Keystream Generators 222
Matthias Krause

Linear Cryptanalysis of Bluetooth Stream Cipher 238
Jovan Dj. Golić, Vittorio Bagini, Guglielmo Morgari

Digital Signatures I

Generic Lower Bounds for Root Extraction and Signature Schemes in General Groups 256
Ivan Damgård, Maciej Koprowski

Optimal Security Proofs for PSS and Other Signature Schemes 272
Jean-Sébastien Coron

Cryptanalysis II

Cryptanalysis of SFLASH 288
Henri Gilbert, Marine Minier

Cryptanalysis of the Revised NTRU Signature Scheme 299
Craig Gentry, Mike Szydlo

Key Exchange

Dynamic Group Diffie-Hellman Key Exchange
under Standard Assumptions 321
Emmanuel Bresson, Olivier Chevassut, David Pointcheval

Universally Composable Notions of Key Exchange and Secure Channels . . . 337
Ran Canetti, Hugo Krawczyk

On Deniability in Quantum Key Exchange 352
Donald Beaver

Modes of Operation

A Practice-Oriented Treatment of Pseudorandom Number Generators 368
Anand Desai, Alejandro Hevia, Yiqun Lisa Yin

A Block-Cipher Mode of Operation
for Parallelizable Message Authentication 384
John Black, Phillip Rogaway

Invited Talk

Rethinking PKI: What's Trust Got to Do with It? 398
Stephen Kent

Digital Signatures II

Efficient Generic Forward-Secure Signatures
with an Unbounded Number of Time Periods 400
Tal Malkin, Daniele Micciancio, Sara Miner

From Identification to Signatures via the Fiat-Shamir Transform:
Minimizing Assumptions for Security and Forward-Security 418
Michel Abdalla, Jee Hea An, Mihir Bellare, Chanathip Namprempre

Security Notions for Unconditionally Secure Signature Schemes 434
Junji Shikata, Goichiro Hanaoka, Yuliang Zheng, Hideki Imai

Traitor Tracking & Id-Based Encryption

Traitor Tracing with Constant Transmission Rate 450
Aggelos Kiayias, Moti Yung

Toward Hierarchical Identity-Based Encryption 466
Jeremy Horwitz, Ben Lynn

Multiparty and Multicast

Unconditional Byzantine Agreement and Multi-party Computation
Secure against Dishonest Minorities from Scratch 482
Matthias Fitzi, Nicolas Gisin, Ueli Maurer, Oliver von Rotz

Perfectly Secure Message Transmission Revisited 502
Yvo Desmedt, Yongge Wang

Symmetric Cryptology

Degree of Composition of Highly Nonlinear Functions
and Applications to Higher Order Differential Cryptanalysis 518
Anne Canteaut, Marion Videau

Security Flaws Induced by CBC Padding –
Applications to SSL, IPSEC, WTLS 534
Serge Vaudenay

Author Index 547