Advances in Cryptology - EUROCRYPT 2002


Bearbeitet von
Lars Knudsen

1. Auflage 2002. Taschenbuch. xii, 552 S. Paperback
ISBN 978 3 540 43553 2
Format (B x L): 15,5 x 23,5 cm
Gewicht: 1720 g

Weitere Fachgebiete > EDV, Informatik > Datenbanken, Informationssicherheit, Geschäftssoftware > Informations- und Kodierungstheorie

Zu Inhaltsverzeichnis

schnell und portofrei erhältlich bei

beck-shop.de
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 Three additional submissions were withdrawn by the authors shortly after the submission deadline.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.

My work as program chair was made a lot easier by the electronic submission software written by Chanathip Namprempre for Crypto2000 with modifications by Andre Adelsbach for Eurocrypt2001, 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 Premeel ...................................................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