Lecture Notes in Computer Science 3027

Commenced Publication in 1973
Founding and Former Series Editors:
Gerhard Goos, Juris Hartmanis, and Jan van Leeuwen

Springer
Berlin
Heidelberg
New York
Hong Kong
London
Milan
Paris
Tokyo

Christian Cachin Jan Camenisch (Eds.)

Advances in Cryptology - EUROCRYPT 2004

International Conference on the Theory
and Applications of Cryptographic Techniques
Interlaken, Switzerland, May 2-6, 2004
Proceedings

Springer

Volume Editors

Christian Cachin
Jan Camenisch
IBM Zurich Research Laboratory
Säumerstrasse 4, CH-8803 Rüschlikon, Switzerland
E-mail: {cca,jca}@zurich.ibm.com

Library of Congress Control Number: Applied for

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

ISSN 0302-9743
ISBN 3-540-21935-8 Springer-Verlag Berlin Heidelberg New York

Typesetting: Camera-ready by author, data conversion by Boller Mediendesign
Printed on acid-free paper SPIN: 10999516 06/3142 5 4 3 2 1 0

Preface

These are the proceedings of Eurocrypt 2004, the 23rd Annual Eurocrypt Conference. The conference was organized by members of the IBM Zurich Research Laboratory in cooperation with IACR, the International Association for Cryptologic Research.

The conference received a record number of 206 submissions, out of which the program committee selected 36 for presentation at the conference (three papers were withdrawn by the authors shortly after submission). These proceedings contain revised versions of the accepted papers. These revisions have not been checked for correctness, and the authors bear full responsibility for the contents of their papers.

The conference program also featured two invited talks. The first one was the 2004 IACR Distinguished Lecture given by Whitfield Diffie. The second invited talk was by Ivan Damgård who presented "Paradigms for Multiparty Computation." The traditional rump session with short informal talks on recent results was chaired by Arjen Lenstra.

The reviewing process was a challenging task, and many good submissions had to be rejected. Each paper was reviewed independently by at least three members of the program committee, and papers co-authored by a member of the program committee were reviewed by at least six (other) members. The individual reviewing phase was followed by profound and sometimes lively discussions about the papers, which contributed a lot to the quality of the final selection. Extensive comments were sent to the authors in most cases. At the end, the comments and electronic discussion notes filled more than 32,000 lines of text! We would like to thank the members of the program committee for their hard work over the course of several months; it was a pleasure for us to work with them and to benefit from their knowledge and insight. We are also very grateful to the external reviewers who contributed with their expertise to the selection process. Their work is highly appreciated.

The submission of all papers was done using the electronic submission software written by Chanathip Namprempre with modifications by Andre Adelsbach. During the review process, the program committee was mainly communicating using the Web-based review software developed by Bart Preneel, Wim Moreau, and Joris Claessens. We would like to thank Roger Zimmermann for his help with installing and running the software locally, and for solving many other problems, not the least of which was the assembly of these proceedings. The final decisions were made at a meeting in Rüschlikon at the IBM Zurich Research Laboratory. Helga Steimann helped us with the organization and also made sure there was enough coffee and food available so that we could concentrate on the papers and were not distracted by empty stomachs. Thanks a lot!

We are grateful to Endre Bangerter, Martin Hirt, Reto Strobl, and Roger Zimmermann for their help with the local arrangements of the conference.

Eurocrypt 2004 was supported by the IBM Zurich Research Laboratory, Crypto AG, Omnisec, MediaCrypt, HP, Microsoft Research, and Swiss International Air Lines.

Our most important thanks go to our families for bearing with us through this busy period, for their support, and for their love.

Last but not least, we thank all the authors from all over the world who submitted papers. It is due to them and their work that the conference took place.

February 2004 Christian Cachin and Jan Camenisch

EUROCRYPT 2004

May 2–6, 2004, Interlaken, Switzerland

Sponsored by the
International Association for Cryptologic Research (*IACR*)

in cooperation with the
IBM Zurich Research Laboratory, Switzerland

Program and General Chairs

Christian Cachin and Jan Camenisch
IBM Zurich Research Laboratory, Switzerland

Program Committee

Alex Biryukov ..... Katholieke Universiteit Leuven, Belgium
John Black ..... University of Colorado at Boulder, USA
Christian Cachin ..... IBM Zurich Research Laboratory, Switzerland
Jan Camenisch ..... IBM Zurich Research Laboratory, Switzerland
Jean-Sébastien Coron ..... Gemplus Card International, France
Claude Crépeau ..... McGill University, Canada
Ivan Damgård ..... Aarhus University, Denmark
Juan Garay ..... Bell Labs - Lucent Technologies, USA
Rosario Gennaro ..... IBM T.J. Watson Research Center, USA
Alain Hiltgen ..... UBS, Switzerland
Thomas Johansson ..... Lund University, Sweden
Antoine Joux ..... DCSSI Crypto Lab, France
Joe Kilian ..... NEC Laboratories America, USA
Arjen Lenstra ..... Citibank, USA & TU Eindhoven, The Netherlands
Yehuda Lindell ..... IBM T.J. Watson Research Center, USA
Anna Lysyanskaya ..... Brown University, USA
Daniele Micciancio ..... UC San Diego, USA
Omer Reingold ..... Weizmann Institute of Science, Israel
Vincent Rijmen ..... Cryptomathic and IAIK, Belgium
Phillip Rogaway ..... UC Davis, USA & Chiang Mai University, Thailand
Igor Shparlinski ..... Macquarie University, Australia
Edlyn Teske ..... University of Waterloo, Canada
Rebecca Wright ..... Stevens Institute of Technology, USA

External Reviewers

Adi Akavia
Joy Algesheimer
Jee Hea An
Siddhartha Annapureddy
Giuseppe Ateniese
Endre Bangerter
Lejla Batina
Amos Beimel
Mihir Bellare
Siddika Berna Ors
Simon Blackburn
Carlo Blundo
Alexandra Boldyreva
Dan Boneh
Colin Boyd
Xavier Boyen
An Braeken
Thomas Brochman
Ran Canetti
Scott Contini
Don Coppersmith
Nora Dabbous
Christophe De Cannière
Alex Dent
Giovanni Di Crescenzo
Christophe Doche
Yevgeniy Dodis
Patrik Ekdahl
Nelly Fazio
Serge Fehr
Marc Fischlin
Matthias Fitzi
Scott Fluhrer
Matt Franklin
Martin Gagne
Steven Galbraith
M. I. Gonzáles Vasco
Jens Groth
Jaime Gutierrez
Stuart Haber
Shai Halevi
Helena Handschuh
Darrel Hankerson
Danny Harnik
Jonathan Herzog
Florian Hess
Alejandro Hevia
Jason Hinek
Susan Hohenberger
Nicholas Hopper
Nick Howgrave-Graham
Jim Hughes
Yuval Ishai
Markus Jakobsson
Stas Jarecki
Eliane Jaulmes
Fredrik Jönsson
Marc Joye
Yael Tauman Kalai
Aggelos Kiayias
Neal Koblitz
David Kohel
Yoshi Kohno
Hugo Krawczyk
Ted Krovetz
Sébastien Kunz-Jacques
John Langford
Joseph Lano
Moses Liskov
Benjamin Lynn
Philip MacKenzie
Chip Martel
Alex May
Dominic Mayers
Ralph C. Merkle
Sara Miner
Ilya Mironov
Siguna Müller
Frédéric Muller
Sean Murphy
Chanathip Namprempre
Moni Naor
Mats Näslund
Phong Nguyen
Antonio Nicolosi
Svetla Nikova
Kobbi Nissim
Luke O'Connor
Roberto Oliveira
Pascal Paillier
Adriana Palacio
Kenneth Paterson
Souradyuti Paul
Thomas Pedersen
Chris Peikert
Erez Petrank
Birgit Pfitzmann
Benny Pinkas
David Pointcheval
Jonathan Poritz
John Proos
Michael Quisquater
Tal Rabin
Zulfikar Ramzan
Leonid Reyzin
Pierre-Michel Ricordel
Alon Rosen
Amit Sahai
Louis Salvail
Palash Sarkar
Jasper Scholten
Hovav Shacham
Taizo Shirai
Thomas Shrimpton
Alice Silverberg
Adam Smith
Patrick Solè
Jessica Staddon
Markus Stadler
Martijn Stam
Andreas Stein
Ron Steinfeld
Reto Strobl
Frédéric Valette
Bart Van Rompay
Luis von Ahn
Shabsi Walfish
Huaxiong Wang
Bogdan Warinschi
John Watrous
Christopher Wolf
Ke Yang

Table of Contents

Foundations I

Identity-Based Encryption

Elliptic Curves

Signatures II

Public-Key Cryptography

Foundations II

Multiparty Computation

Cryptanalysis

New Applications

Algorithms and Implementation

Anonymity