

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206 submissions, out of which the program committee selected 36 for presentation at the conference (three papers were withdrawn by the authors shortly after submission).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	Jonathan Herzog	Roberto Oliveira
Joy Algesheimer	Florian Hess	Pascal Paillier
Jee Hea An	Alejandro Hevia	Adriana Palacio
Siddhartha Annapureddy	Jason Hinek	Kenneth Paterson
Giuseppe Ateniese	Susan Hohenberger	Souradyuti Paul
Endre Bangerter	Nicholas Hopper	Thomas Pedersen
Lejla Batina	Nick Howgrave-Graham	Chris Peikert
Amos Beimel	Jim Hughes	Erez Petrank
Mihir Bellare	Yuval Ishai	Birgit Pfitzmann
Siddika Berna Ors	Markus Jakobsson	Benny Pinkas
Simon Blackburn	Stas Jarecki	David Pointcheval
Carlo Blundo	Eliane Jaulmes	Jonathan Poritz
Alexandra Boldyreva	Fredrik Jönsson	John Proos
Dan Boneh	Marc Joye	Michael Quisquater
Colin Boyd	Yael Tauman Kalai	Tal Rabin
Xavier Boyen	Aggelos Kiayias	Zulfikar Ramzan
An Braeken	Neal Koblitz	Leonid Reyzin
Thomas Brochman	David Kohel	Pierre-Michel Ricordel
Ran Canetti	Yoshi Kohno	Alon Rosen
Scott Contini	Hugo Krawczyk	Amit Sahai
Don Coppersmith	Ted Krovetz	Louis Salvail
Nora Dabbous	Sébastien Kunz-Jacques	Palash Sarkar
Christophe De Cannière	John Langford	Jasper Scholten
Alex Dent	Joseph Lano	Hovav Shacham
Giovanni Di Crescenzo	Moses Liskov	Taizo Shirai
Christophe Doche	Benjamin Lynn	Thomas Shrimpton
Yevgeniy Dodis	Philip MacKenzie	Alice Silverberg
Patrik Ekdahl	Chip Martel	Adam Smith
Nelly Fazio	Alex May	Patrick Solè
Serge Fehr	Dominic Mayers	Jessica Staddon
Marc Fischlin	Ralph C. Merkle	Markus Stadler
Matthias Fitzi	Sara Miner	Martijn Stam
Scott Fluhrer	Ilya Mironov	Andreas Stein
Matt Franklin	Siguna Müller	Ron Steinfeld
Martin Gagne	Frédéric Muller	Reto Strobl
Steven Galbraith	Sean Murphy	Frédéric Valette
M. I. Gonzáles Vasco	Chanathip Namprempre	Bart Van Rompay
Jens Groth	Moni Naor	Luis von Ahn
Jaime Gutierrez	Mats Näslund	Shabsi Walfish
Stuart Haber	Phong Nguyen	Huaxiong Wang
Shai Halevi	Antonio Nicolosi	Bogdan Warinschi
Helena Handschuh	Svetla Nikova	John Watrous
Darrel Hankerson	Kobbi Nissim	Christopher Wolf
Danny Harnik	Luke O'Connor	Ke Yang

Advances in Cryptology - EUROCRYPT 2004
International Conference on the Theory and
Applications of Cryptographic Techniques, Interlaken,
Switzerland, May 2-6, 2004. Proceedings
Cachin, C.; Camensich, J. (Eds.)
2004, XII, 630 p., Softcover
ISBN: 978-3-540-21935-4