Preface

EUROCRYPT 2000, the nineteenth annual Eurocrypt Conference, was sponsored by the International Association for Cryptologic Research (IACR), in cooperation with the Katholieke Universiteit Leuven in Belgium (research group for Computer Security and Industrial Cryptography, COSIC).

The first conference with the name 'Eurocrypt' took place in 1983, but the 1982 Workshop at Burg Feuerstein was the first open meeting in Europe on cryptology; it has been included in Lecture Notes in Computer Science 1440, which contains an electronic proceedings and index of the Crypto and Eurocrypt conferences 1981–1997.

The program committee considered 150 papers and selected 39 for presentation at EUROCRYPT 2000. One paper was withdrawn by the authors. The program also included invited talks by Michael Walker ("On the Security of 3GPP Networks") and Tony Sale ("Colossus and the German Lorenz Cipher – Code Breaking in WW II"). In addition, Andy Clark kindly agreed to chair the traditional rump session for informal presentations of recent results.

The selection of the program was a challenging task, as many high quality submissions were received. Each submission was reviewed by at least three reviewers and most reports had four or more reviews (papers with program committee members as a co-author had at least six reviews). The program committee worked very hard to evaluate the papers with respect to quality, originality, and relevance to cryptology. In most cases they were able to provide extensive comments to the authors (about half a megabyte of comments for authors has been written). Subsequently, the authors of accepted papers have made a substantial effort to take into account the comments in the version submitted to these proceedings. In a limited number of cases, these revisions have been checked by members of the program committee.

First and foremost I would like to thank the members of the program committee for the many hours spent on reviewing and discussing the papers, and for helping me with the difficult decisions.

I gratefully acknowledge the help of a large number of colleagues who reviewed submissions in their area of expertise: Masayuki Abe, N. Asokan, Olivier Baudron, Josh Benaloh, Eli Biham, Simon Blake-Wilson, Johan Borst, Emmanuel Bresson, Jan Camenisch, Ivan Damgård, Anand Desai, Yvo Desmedt, Glenn Durfee, Serge Fehr, Matthias Fitzi, Pierre-Alain Fouque, Matt Franklin, Steven Galbraith, Juan A. Garay, Louis Granboulan, Stuart Haber, Shai Halevi, Martin Hirt, Fredrik Jönsson, Mike Jacobson, Jens G. Jensen, Ari Juels, Jonathan Katz, Robert Lambert, Julio Lopez Hernandez, Phil MacKenzie, Julien Marcil, Willi Meier, Preda Mihailescu, Serge Mister, Fabian Monrose, Sean Murphy, Siaw-Lynn Ng, Phong Nguyen, Valtteri Niemi, Tatsuaki Okamoto, Thomas

Pornin, Guillaume Poupard, Bartek Przydatek, Omer Reingold, Vincent Rijmen, Louis Salvail, Tomas Sander, Berry Schoenmakers, Dan Simon, Ben Smeets, Michael Steiner, Jacques Stern, Martin Strauss, Katsuyuki Takashima, Edlyn Teske, Barry Trager, Ramarathnam Venkatesan, Frederik Vercauteren, Susanne Wetzel, Mike Wiener, Peter Wild, Adam Young. I apologise for any inadvertent omissions.

By now, electronic submissions have become a tradition for Eurocrypt. I would like to thank Joe Kilian, who did an excellent job in running the electronic submission server of ACM's SIGACT group. Only five contributions were submitted in paper form; for three of these, I obtained an electronic copy from the authors. The remaining two papers were scanned in to make the process uniform to reviewers. As a first for IACR sponsored conferences, we developed a web interface for entering reviews and discussing papers. Special thanks go to Joris Claessens and Wim Moreau who spent several weeks developing my rough specifications into a flawless program with a smooth user interface. This work made the job of the program committee much easier, as we could focus on the content of the discussion rather than on its organization. This software will be made available to all IACR sponsored conferences.

My ability to run the program committee was increased substantially by the effort and skills provided by the members of COSIC: Vincent Rijmen put together the LaTeX version of the proceedings, Joris Claessens helped with processing the submissions, Johan Borst converted a paper to LaTeX, Péla Noë assisted with organizing the program committee meeting, and (last but not least) Wim Moreau helped with the electronic processing of the submissions and final versions, and with the copyright forms.

I would like to thank Joos Vandewalle, general chair, the members of the organizing committee (Joris Claessens, Danny De Cock, Erik De Win, Marijke De Soete, Keith Martin, Wim Moreau, Péla Noë, Jean-Jacques Quisquater, Vincent Rijmen, Bart Van Rompay, Karel Wouters), and the other members of COSIC for their support. I also thank Elvira Wouters, who took care of the accounting, and Anne De Smet (Momentum), who was responsible for the hotel bookings and the social program. For the first time, the registrations of Eurocrypt were handled by the IACR General Secretariat in Santa Barbara (UCSB); I would like to thank Micky Swick and Sally Vito for the successful collaboration. The organizing committee gratefully acknowledges the financial contributions of our sponsors: Isabel, Ubizen, Europay International, Cryptomathic Belgium, PriceWaterhouseCoopers, Utimaco, and the Katholieke Universiteit Leuven.

Finally, I wish to thank all the authors who submitted papers, making this conference possible, and the authors of accepted papers for their cooperation. Special thanks go to Alfred Hofmann and his colleagues at Springer-Verlag for the timely production of this volume.

March 2000 Bart Preneel

EUROCRYPT 2000

May 14–18, 2000, Bruges, Belgium

Sponsored by the
International Association for Cryptologic Research

General Chair

Joos Vandewalle, Katholieke Universiteit Leuven, Belgium

Program Chair

Bart Preneel, Katholieke Universiteit Leuven, Belgium

Program Committee

Simon Blackburn ..... Royal Holloway Univ. of London, UK
Dan Boneh ..... Stanford Univ., USA
Christian Cachin ..... IBM Research, Switzerland
Don Coppersmith ..... IBM Research, USA
Ronald Cramer ..... ETH Zurich, Switzerland
Hans Dobbertin ..... BSI, Germany
Markus Jakobsson ..... Bell Laboratories, USA
Thomas Johansson ..... Lund Univ., Sweden
Joe Kilian ..... NEC Research Institute, USA
Lars Knudsen ..... Univ. of Bergen, Norway
Mitsuru Matsui ..... Mitsubishi, Japan
Alfred Menezes ..... Univ. of Waterloo, Canada
Moni Naor ..... Weizmann Institute of Science, Israel
Kaisa Nyberg ..... Nokia Research Center, Finland
Paul van Oorschot ..... Entrust Technologies, Canada
Torben Pedersen ..... Cryptomathic, Denmark
David Pointcheval ..... ENS, France
Moti Yung ..... Certco, USA