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 organisation, 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 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 merge 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 Three additional submissions were withdrawn by the authors shortly after the submission deadline.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 to the authors were produced. 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 finalised with a meeting in Copenhagen January 13th, 2002.

I'm 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 a 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'd like to thank Ole da Silva Smith for setting up all this software locally and for the help with the problems I encountered. Also thank you 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 to 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 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