Preface

The EUROCRYPT '98 conference was organized and sponsored by the International Association for Cryptologic Research in cooperation with and hosted by the Helsinki University of Technology. It took place at the university campus in Espoo, Finland, May 31–June 4, 1998. This year was also the 100th birthday of architect Alvar Aalto, the designer of the Main Hall of the University of Technology where the presentations the 17th annual EUROCRYPT conference were held. Professor Arto Karila, the General Chair, was responsible for local organization. His contribution to the success of the conference is gratefully acknowledged. I would also like to thank Tuomas Aura for managing practical arrangements and creating and maintaining the conference website.

The scientific program for EUROCRYPT '98 was put together by an 18-member program committee which considered 161 submissions by researchers from all over the world. The quality of the submissions was exceptionally high, as is reflected in the number of contributions published in these proceedings, which contain the revised versions of 44 papers accepted for presentation. Still, many good papers had to be left out.

I would like to thank the members of the program committee who devoted an enormous amount of time and energy to reading the papers and making the difficult selection. In addition, I gratefully acknowledge the support to the program commitee by the following experts: Klaus Becker, Simon Blackburn, Daniel Bleichenbacher, Antoon Bosselaers, Karl Brincat, Mike Burmester, Claude Carlet, Cunsheng Ding, DengGuo Feng, Steven Galbraith, Mika Hirvensalo, Shao-Quan Jiang, Juhani Karhumäki, Lars Knudsen, Kaoru Kurosawa, Keith Martin, Alexandru Mateescu, Willi Meier, Tommi Meskanen, Chris Mitchell, Thomas Mittelholzer, Sean Murphy, Phong Nguyen, Kazuo Ohta, Eiji Okamoto, Tatsuaki Okamoto, René Peralta, Holger Petersen, Andreas Pfitzmann, Josef Pieprzyk, Thomas Pornin, Guillaume Poupard, Ari Renvall, Vincent Rijmen, Ahmad-Reza Sadeghi, Kazue Sako, Ruediger Schack, Matthias Schunter, Jacques Stern, Douglas Stinson, Keisuke Tanaka, Michael Waidner, Uta Wille, Qibin Zhai, Xianmo Zhang, Junhui Yang, DingFeng Ye, and Øyvind Ytrehus.

Finally, I would like to thank all authors who submitted papers to EUROCRYPT '98 and, in particular, the authors of the accepted papers for their cooperation in producing these proceedings.

March 1998 Kaisa Nyberg

Eurocrypt '98

May 31–June 4, 1998, Espoo, Finland

Sponsored by the

International Association for Cryptologic Research (IACR)

General Chair

Arto Karila, Helsinki University of Technology, Finland

Program Chair

Kaisa Nyberg, Finnish Defence Forces, Finland

Program Committee

Zongduo Dai . . . . . Academia Sinica, China
Yvo Desmedt . . . . . University of Wisconsin, USA
Hans Dobbertin . . . . . BSI, Germany
Dieter Gollman . . . . . Microsoft, U.K.
Tor Helleseth . . . . . University of Bergen, Norway
Markus Jakobsson . . . . . Bell Labs, USA
Thomas Johansson . . . . . University of Lund, Sweden
Xueija Lai . . . . . R3 Security Engineering AG, Switzerland
Arjen K. Lenstra . . . . . Citibank, USA
Mitsuru Matsui . . . . . Mitsubishi, Japan
Torben Pedersen . . . . . Cryptomathic, Denmark
Birgit Pfitzmann . . . . . University of Saarland, Germany
Bart Preneel . . . . . K.U.Leuven, Belgium
Rei Safavi-Naini . . . . . University of Wollongong, Australia
Arto Salomaa . . . . . University of Turku, Finland
Othmar Staffelbach . . . . . .UG FU, Switzerland
Serge Vaudenay . . . . . Ecole Normale Supérieure, France
Moti Yung . . . . . CertCo, USA