

Preface

EUROCRYPT 2001, the 20th annual Eurocrypt conference, was sponsored by the IACR, the International Association for Cryptologic Research, see <http://www.iacr.org/>, this year in cooperation with the Austrian Computer Society (OCG). The General Chair, Reinhard Posch, was responsible for local organization, and registration was handled by the IACR Secretariat at the University of California, Santa Barbara.

In addition to the papers contained in these proceedings, we were pleased that the conference program also included a presentation by the 2001 IACR distinguished lecturer, Andrew Odlyzko, on “Economics and Cryptography” and an invited talk by Silvio Micali, “Zero Knowledge Has Come of Age.” Furthermore, there was the rump session for presentations of recent results and other (possibly satirical) topics of interest to the crypto community, which Jean-Jacques Quisquater kindly agreed to run.

The Program Committee received 155 submissions and selected 33 papers for presentation; one of them was withdrawn by the authors. The review process was therefore a delicate and challenging task for the committee members, and I wish to thank them for all the effort they spent on it. Each committee member was responsible for the review of at least 20 submissions, so each paper was carefully evaluated by at least three reviewers, and submissions with a program committee member as a (co-)author by at least six. Final decisions, after intensive web discussions, were taken at a one-day face-to-face program committee meeting. The selection was based on originality, quality, and relevance to cryptography. In most cases, the reviewers provided extensive comments to the authors. Subsequently, the authors made a substantial effort to take these comments into account. I was pleased to see that the field is continuing to flourish and believe that we were able to select a varied and high-quality program. I wish to thank all the authors who submitted papers, thus making such a choice possible, and those of accepted papers for their cooperation in the timely production of revised versions.

Many thanks also go to the additional colleagues who reviewed submissions in their area of expertise: Joy Algesheimer, Seigo Arita, Giuseppe Ateniese, Olivier Baudron, Charles Bennett, Dan Boneh, Annalisa De Bonis, Wieb Bosma, Marco Bucci, Ran Canetti, Anne Canteaut, Suresh Chari, Philippe Chose, Christophe Clavier, Scott Contini, Don Coppersmith, Jean-Sébastien Coron, Ronald Cramer, Nora Dabbous, Ivan Damgård, Giovanni Di Crescenzo, Markus Dichtl, Yevgeniy Dodis, Paul Dumais, Serge Fehr, Marc Fischlin, Roger Fischlin, Matthias Fitzi, Pierre-Alain Fouque, Jun Furukawa, Pierre Girard, Clemente Gladi, Daniel Gottesman, Clemens Holenstein, Rosario Gennaro, Nick Howgrave-Graham, James Hughes, Yuval Ishai, Markus Jakobsson, Eliane Jaulmes, Antoine Joux, Olaf Keller, Ki Hyoung Ko, Reto Kohlas, Takeshi Koshihara, Eyal Kushilevitz, Yehuda Lindell, Helger Lipmaa, Anna Lysyanskaya, Subhamoy

Maitra, Tal Malkin, Daniel Mall, Barbara Masucci, Dominic Mayers, Alfred Menezes, Renato Menicocci, Daniele Micciancio, Markus Michels, Miodrag Mihaljevic, Phong Nguyen, Svetla Nikova, Satoshi Obana, Kazuo Ohta, Pino Persiano, David Pointcheval, Bartosz Przydatek, Michael Quisquater, Omer Reingold, Leonid Reyzin, Jean-Marc Robert, Pankaj Rohatgi, Alon Rosen, Ludovic Rousseau, Daniel Simon, Nigel Smart, Adam Smith, Othmar Staffelbach, Martijn Stam, Michael Steiner, Katsuyuki Takashima, Alain Tapp, Christophe Tychmen, Shigenori Uchiyama, Frédéric Valette, Ramarathnam Venkatesan, Eric Verheul, Stefan Wolf, Akihiro Yamamura, Yuliang Zheng. I apologize for any inadvertent omissions.

The review process was greatly simplified by submission software written by Mihir Bellare and Chanathip Namprempre for Crypto 2000, and review software developed for EUROCRYPT 2000 by Bart Preneel, Wim Moreau, and Joris Claessens.

I am very grateful to André Adelsbach. Skillfully and patiently, he carried the main load of background work of the Program Chair, in particular in setting up the submission and review servers, providing technical help to the authors and committee members, and in the preparation of these proceedings. I would also like to thank Michael Steiner and Martin Wanke for technical support, Matthias Schunter for organizing the program committee meeting, and Mihir Bellare and Michael Waidner for advice.

March 2001

Birgit Pfitzmann

EUROCRYPT 2001

May 6 – 10, 2001, Innsbruck (Tyrol), Austria

Sponsored by the
International Association for Cryptologic Research (IACR)
in cooperation with the
Austrian Computer Society (OCG)

General Chair

Reinhard Posch, Institute for Applied Information Processing and
Communications (IAIK), Austria

Program Chair

Birgit Pfitzmann, Saarland University, Saarbrücken, Germany

Program Committee

Josh Benaloh	Microsoft Research, USA
Carlo Blundo	Università di Salerno, Italy
Jan Camenisch	IBM Zürich Research Laboratory, Switzerland
Matt Franklin	UC Davis, USA
Shai Halevi	IBM T. J. Watson Research Center, USA
Martin Hirt	ETH Zürich, Switzerland
Thomas Johansson	Lund University, Sweden
Neal Koblitz	Univ. of Washington, USA
Hugo Krawczyk	Technion, Israel
Kaoru Kurosawa	Tokyo Institute of Technology, Japan
Arjen Lenstra	Citicorp, USA
Willi Meier	Fachhochschule Aargau, Switzerland
David Naccache	Gemplus, France
Kaisa Nyberg	Nokia, Finland
Torben Pryds Pedersen	Cryptomathic, Denmark
Guillaume Poupard	DCSSI Crypto Lab, France
Tal Rabin	IBM T. J. Watson Research Center, USA
Vincent Rijmen	K. U. Leuven, Belgium
Amit Sahai	Princeton University, USA
Kazue Sako	NEC, Japan
Louis Salvail	BRICS, University of Århus, Denmark
Claus-Peter Schnorr	University of Frankfurt, Germany
David Wagner	UC Berkeley, USA
Michael Waidner	IBM Zürich Research Laboratory, Switzerland

Advances in Cryptology - EUROCRYPT 2001
International Conference on the Theory and Application
of Cryptographic Techniques Innsbruck, Austria, May
6-10, 2001, Proceedings
Pfitzmann, B. (Ed.)
2001, XIII, 544 p. 23 illus., Softcover
ISBN: 978-3-540-42070-5