Preface

Crypto '99, the Nineteenth Annual Crypto Conference, was sponsored by the International Association for Cryptologic Research (IACR), in cooperation with the IEEE Computer Society Technical Committee on Security and Privacy and the Computer Science Department, University of California, Santa Barbara (UCSB). The General Chair, Donald Beaver, was responsible for local organization and registration.

The Program Committee considered 167 papers and selected 38 for presentation. This year's conference program also included two invited lectures. I was pleased to include in the program Ueli Maurer's presentation "Information-Theoretic Cryptography" and Martin Hellman's presentation "The Evolution of Public-Key Cryptography." The program also incorporated the traditional Rump Session for informal short presentations of new results, run by Stuart Haber.

These proceedings include the revised versions of the 38 papers accepted by the Program Committee. These papers were selected from all the submissions to the conference based on originality, quality, and relevance to the field of cryptology. Revisions were not checked, and the authors bear full responsibility for the contents of their papers.

The selection of papers was a difficult and challenging task. I wish to thank the Program Committee members who did an excellent job in reviewing papers and providing useful feedback to authors. Each submission was refereed by at least three reviewers. The Program Committee was assisted by many colleagues who reviewed submissions in their areas of expertise. My thanks go to all of them. External Reviewers included Michel Abdalla, Masayuki Abe, Bill Aiello, Kazumaro Aoki, Olivier Baudron, Don Beaver, Josh Benaloh, John Black, Simon Blackburn, Carlo Blundo, Dan Boneh, Johan Borst, Antoon Bosselaers, Christian Cachin, Jan Camenisch, Ran Canetti, Suresh Chari, Jean-Sébastien Coron, Janos Csirik, Erik De Win, Giovanni Di Crescenzo, Serge Fehr, Matthias Fitzi, Matt Franklin, Atsushi Fujioka, Juan Garay, Louis Granboulan, Shai Halevi, Héléna Handschuh, Kim Harrison, Martin Hirt, Russell Impagliazzo, Markus Jakobsson, Mariusz Jakubowski, Thomas Johansson, Marc Joye, Ari Juels, Charanjit Jutla, Burt Kaliski, Masayuki Kanda, Olaf Keller, Kunio Kobayashi, Tetsutaro Kobayashi, Ted Krovetz, Eyal Kushilevitz, Yue Lai, Susan Langford, Yishay Mansour, Keith Martin, Jim Massey, Phil MacKenzie, Andrew Mertz, Markus Michels, Victor Miller, Shiho Moriai, David Naccache, Moni Naor, Phong Nguyen, Tatsuaki Okamoto, Carles Padró, Pascal Paillier, Benny Pinkas, David Pointcheval, Guillaume Poupard, Vincent Rijmen, Kazue Sako, Kouichi Sakurai, Louis Salvail, Berry Schoenmakers, Nigel Smart, Jessica Staddon, Jacques Stern, Julien P. Stern, Douglas Stinson, Stuart Stubblebine, Youici Takasima, Keisuke Tanaka, Shigenori Uchiyama, Salil Vadhan, Ramarathnam Venkatesan, Ruizhong Wei, Avishai Wool, Yacov Yacobi, Lisa Yin, and Adam Young. I apologize for any inadvertent omissions.

The practice of accepting submissions electronically was continued for Crypto '99. Authors chose the electronic submission option for all but four papers. All credit for

the smooth electronic submission process goes to Joe Kilian, who handled all aspects and delivered a convenient directory full of submissions.

In organizing the scientific program and putting together these proceedings, I have been assisted by many people in addition to those mentioned above. In particular, I'd like to thank: Hugo Krawczyk, the Program Chair for Crypto '98, for his good advice and patience in answering my many questions; Don Coppersmith for his help throughout the review process; Donald Beaver, the General Chair of the conference, for freeing me from all issues not directly related to the scientific program and proceedings; Serge Mister for editing postscript submissions so that they would view and print acceptably; and Debbie Morton for secretarial help, particularly in helping to organize the Program Committee meeting.

Finally, I wish to thank all the authors who submitted papers, making this conference possible, and the authors of accepted papers for updating their papers in a timely fashion, allowing the production of these proceedings.

June 1999

Michael J. Wiener
Program Chair

CRYPTO '99

August 15-19, 1999, Santa Barbara, California, USA

Sponsored by the

International Association for Cryptologic Research (IACR)

in cooperation with

IEEE Computer Society Technical Committee on Security and Privacy,
Computer Science Department, University of California, Santa Barbara

General Chair

Donald Beaver, CertCo, USA

Program Chair

Michael J. Wiener, Entrust Technologies, Canada

Program Committee

Daniel Bleichenbacher ..... Bell Laboratories, USA
Don Coppersmith ..... IBM Research, USA
Ivan Damgård ..... Aarhus University, Denmark
Ronald Cramer ..... ETH Zurich, Switzerland
Rosario Gennaro ..... IBM Research, USA
Andrew Klapper ..... University of Kentucky, USA
Lars Knudsen ..... University of Bergen, Norway
Xuejia Lai ..... r^3 security engineering, Switzerland
Arjen Lenstra ..... Citibank, USA
Andrew Odlyzko ..... AT&T Labs - Research, USA
Kazuo Ohta ..... NTT Lab., Japan
Bart Preneel ..... Katholieke Universiteit Leuven, Belgium
Jean-Jacques Quisquater ..... Université Catholique de Louvain, Belgium
Matt Robshaw ..... RSA Laboratories, USA
Phillip Rogaway ..... University of California at Davis, USA
Daniel Simon ..... Microsoft Research, USA
Serge Vaudenay ..... Ecole Normale Supérieure, France
Moti Yung ..... CertCo, USA

Advisory Members

Mihir Bellare (Crypto 2000 Program Chair) . University of California at San Diego, USA
Joe Kilian (Electronic submissions) ..... NEC Research Institute, USA
Hugo Krawczyk (Crypto '98 Program Chair) ..... Technion, Israel and IBM, USA