Preface

Crypto 2000 was the 20th Annual Crypto conference. It 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 of the University of California at Santa Barbara.

The conference received 120 submissions, and the program committee selected 32 of these for presentation. Extended abstracts of revised versions of these papers are in these proceedings. The authors bear full responsibility for the contents of their papers.

The conference program included two invited lectures. Don Coppersmith's presentation "The development of DES" recorded his involvement with one of the most important cryptographic developments ever, namely the Data Encryption Standard, and was particularly apt given the imminent selection of the Advanced Encryption Standard. Martín Abadi's presentation "Taming the Adversary" was about bridging the gap between useful but perhaps simplistic threat abstractions and rigorous adversarial models, or perhaps, even more generally, between viewpoints of the security and cryptography communities. An abstract corresponding to Martín's talk is included in these proceedings.

The conference program also included its traditional "rump session" of short, informal or impromptu presentations, chaired this time by Stuart Haber. These presentations are not reflected in these proceedings.

An electronic submission process was available and recommended, but for the first time used a web interface rather than email. (Perhaps as a result, there were no hardcopy submissions.) The submission review process had three phases. In the first phase, program committee members compiled reports (assisted at their discretion by sub-referees of their choice, but without interaction with other program committee members) and entered them, via web forms, into web-review software running at UCSD. In the second phase, committee members used the software to browse each other's reports, discuss, and update their own reports. Lastly there was a program committee meeting to discuss the difficult cases.

I am extremely grateful to the program committee members for their enormous investment of time, effort, and adrenaline in the difficult and delicate process of review and selection. (A list of program committee members and sub-referees they invoked can be found on succeeding pages of this volume.) I also thank the authors of submitted papers —in equal measure regardless of whether their papers were accepted or not— for their submissions. It is the work of this body of researchers that makes this conference possible.

I thank Rebecca Wright for hosting the program committee meeting at the AT&T building in New York City and managing the local arrangements, and Ran Canetti for organizing the post-PC-meeting dinner with his characteristic gastronomic and oenophilic flair.

The web-review software we used was written for Eurocrypt 2000 by Wim Moreau and Joris Claessens under the direction of Eurocrypt 2000 program chair Bart Preneel, and I thank them for allowing us to deploy their useful and colorful tool.

I am most grateful to Chanathip Namprempre (aka. Meaw) who provided systems, logistical, and moral support for the entire Crypto 2000 process. She wrote the software for the web-based submissions, adapted and ran the web-review software at UCSD, and compiled the final abstracts into the proceedings you see here. She types faster than I speak.

I am grateful to Hugo Krawczyk for his insight and advice, provided over a long period of time with his usual combination of honesty and charm, and to him and other past program committee chairs, most notably Michael Wiener and Bart Preneel, for replies to the host of questions I posed during the process. In addition I received useful advice from many members of our community including Silvio Micali, Tal Rabin, Ron Rivest, Phil Rogaway, and Adi Shamir. Finally thanks to Matt Franklin who as general chair was in charge of the local organization and finances, and, on the IACR side, to Christian Cachin, Kevin McCurley, and Paul Van Oorschot.

Chairing a Crypto program committee is a learning process. I have come to appreciate even more than before the quality and variety of work in our field, and I hope the papers in this volume contribute further to its development.

June 2000   MIHIR BELLARE
                                                      Program Chair, Crypto 2000

CRYPTO 2000

August 20–24, 2000, 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
Matthew Franklin, Xerox Palo Alto Research Center, USA

Program Chair
Mihir Bellare, University of California, San Diego, USA

Program Committee

Alex Biryukov .... Weizmann Institute of Science, Israel
Dan Boneh .... Stanford University, USA
Christian Cachin .... IBM Research, Switzerland
Ran Canetti .... IBM Research, USA
Ronald Cramer .... ETH Zurich, Switzerland
Yair Frankel .... CertCo, USA
Shai Halevi .... IBM Research, USA
Arjen Lenstra .... Citibank, USA
Mitsuru Matsui .... Mitsubishi Electric Corporation, Japan
Paul Van Oorschot ....Entrust Technologies, Canada
Bart Preneel .... Katholieke Universiteit Leuven, Belgium
Phillip Rogaway .... University of California, Davis, USA
Victor Shoup .... IBM Zurich, Switzerland
Jessica Staddon .... Bell Labs Research, Palo Alto, USA
Jacques Stern .... Ecole Normale Supérieure, France
Doug Stinson .... University of Waterloo, Canada
Salil Vadhan .... Massachusetts Institute of Technology, USA
David Wagner .... University of California, Berkeley, USA
Rebecca Wright .... AT&T Laboratories Research, USA

Advisory members

Michael Wiener (Crypto 1999 program chair) .. Entrust Technologies, Canada
Joe Kilian (Crypto 2001 program chair) .... Intermemory, USA

Sub-Referees

Bill Aiello, Jeehea An, Olivier Baudron, Don Beaver, Josh Benaloh, John Black, Simon Blackburn, Alexandra Boldyreva, Nikita Borisov, Victor Boyko, Jan Camenisch, Suresh Chari, Scott Contini, Don Coppersmith, Claude Crépeau, Ivan Damgård, Anand Desai , Giovanni Di Crescenzo, Yevgeniy Dodis, Matthias Fitzi, Matt Franklin, Rosario Gennaro, Guang Gong, Luis Granboulan, Nick Howgrave-Graham, Russell Impagliazzo, Yuval Ishai, Markus Jakobsson, Stas Jarecki, Thomas Johansson, Charanjit Jutla, Joe Kilian, Eyal Kushilevitz, Moses Liskov, Stefan Lucks, Anna Lysyanskaya, Philip MacKenzie, Subhamoy Maitra, Tal Malkin, Barbara Masucci, Alfred Menezes, Daniele Micciancio, Sara Miner, Ilia Mironov, Moni Naor , Phong Nguyen, Rafail Ostrovsky, Erez Petrank, Birgit Pfitzmann, Benny Pinkas, David Pointcheval, Guillaume Poupard, Tal Rabin, Charlie Rackoff, Zulfikar Ramzan, Omer Reingold, Leo Reyzin, Pankaj Rohatgi, Amit Sahai, Louis Salvail, Claus Schnorr, Mike Semanko, Bob Silverman, Joe Silverman, Dan Simon, Nigel Smart, Ben Smeets, Adam Smith, Martin Strauss, Ganesh Sundaram, Serge Vaudenay, Frederik Vercauteren, Bernhard von Stengel, Ruizhong Wei, Susanne Gudrun Wetzel, Colin Williams, Stefan Wolf, Felix Wu, Yiqun Lisa Yin, Amir Youssef, Robert Zuccherato