

Advances in Cryptology - CRYPTO 2000

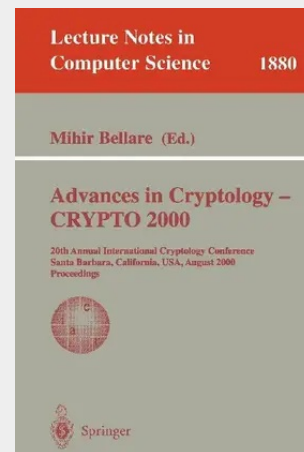
20th Annual International Cryptology Conference, Santa Barbara, California, USA, August 20-24, 2000. Proceedings

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 referees they invoked can be found on succeeding pages of this volume.) I also thank the authors of submitted papers—inequal 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 enophilic flair. VI Preface 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 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 I thank 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



53,49 €
49,99 € (zzgl. MwSt.)

Lieferfrist: bis zu 10 Tage

Artikelnummer: 9783540679073
Medium: Buch
ISBN: 978-3-540-67907-3
Verlag: Springer
Erscheinungstermin: 09.08.2000
Sprache(n): Englisch
Auflage: Erscheinungsjahr 2000
Serie: Lecture Notes in Computer Science
Produktform: Kartoniert
Gewicht: 1720 g
Seiten: 543
Format (B x H): 155 x 235 mm

