CRYPTO 2000

August 20–24, 2000, Santa Barbara, California, USA

CALL FOR PAPERS

URL: `http://www.cse.ucsd.edu/users/mihir/crypto2k`

Original papers on all technical aspects of cryptology are solicited for submission to Crypto 2000, the Twentieth Annual IACR Crypto Conference. Crypto 2000 is organized 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, Santa Barbara. Important Dates are:

Conference	August 20 – 24, 2000
(Electronic) Submission Deadline	February 10, 2000, 17:00 EST
Notification of decision	April 26, 2000
Proceedings version deadline	May 30, 2000

Instructions for authors

Submissions must not substantially duplicate work that any of the authors has published elsewhere or has submitted in parallel to any other conference or workshop that has proceedings.

Submission Format: The paper must be anonymous, with no author names, affiliations, acknowledgments, or obvious references. It should begin with a title, a short abstract, and a list of keywords. The length of the paper should be at most 12 pages excluding bibliography and appendices, and at most 26 pages total. It should use at least 11-point fonts and have reasonable sized margins. The Introduction should summarize the contributions of the paper at a level appropriate for a non-specialist reader. Committee members are not required to read appendices; the paper should be intelligible without them. Submissions not meeting these guidelines risk rejection without consideration of their merits.

Electronic submission: This is strongly encouraged. A detailed description of the electronic submission procedure will appear by January 21, 2000 at

`http://www.cse.ucsd.edu/users/mihir/crypto2k/electronic.html`

Electronic submissions must conform to this procedure and be received by February 10, 2000, 17:00 EST in order to be considered.

Hardcopy submission: Authors unable to submit electronically are invited to send a cover letter and 20 hardcopies of their submission (double-sided) to the Program Chair at the postal address below. Submissions must be received by the Program Chair on or before February 02, 2000 (or postmarked by January 28, 2000, and sent via airmail or courier). Late submissions and submissions by fax will not be considered. The cover letter should contain the paper's title and the names and affiliations of the authors, and should identify the contact author including e-mail and postal addresses.

Decisions and presentation: Notification of acceptance or rejection will be sent to authors by April 26, 2000. Authors of accepted papers must guarantee that their paper will be presented at the conference.

Conference Proceedings: Proceedings will be published in Springer-Verlag's Lecture Notes in Computer Science and will be available at the conference. Clear instructions about the preparation of a final proceedings version will be sent to the authors of accepted papers. The final copies of the accepted papers will be due on May 30, 2000.

Program Committee

Mihir Bellare, Program Chair	University of California, San Diego
Alex Biryukov	Weizmann Institute of Science
Dan Boneh	Stanford University
Christian Cachin	IBM Zurich
Ran Canetti	IBM T.J. Watson
Ronald Cramer	ETH Zurich
Yair Frankel	CertCo
Shai Halevi	IBM T.J. Watson
Arjen Lenstra	Citibank
Mitsuru Matsui	Mitsubishi
Paul Van Oorschot	Entrust
Bart Preneel	Katholieke Universiteit Leuven
Phillip Rogaway	University of California, Davis
Victor Shoup	IBM Zurich
Jessica Staddon	Bell Labs, Palo Alto
Jacques Stern	Ecole Normale Superieure, Paris
Doug Stinson	University of Waterloo
Salil Vadhan	Massachusetts Institute of Technology
David Wagner	University of California, Berkeley
Rebecca Wright	AT&T Laboratories

Advisory members: Michael Wiener (Entrust, Crypto 1999 program chair) and Joe Kilian (NEC, Crypto 2001 program chair).

Contact Information for Program Chair

Mihir Bellare, Program Chair, Crypto 2000

Department of Computer Science and Engineering 0114, AP&M Bldg Room 4230, University of California at San Diego, 9500 Gilman Drive, La Jolla, CA 92093-0114, USA

Phone: 858-534-4544 ; **FAX:** 858-534-7029 ; **E-mail:** mihir@cs.ucsd.edu

Other Information

For other information contact

Mathew Franklin, General Chair, Crypto 2000

Xerox Parc, 3333 Coyote Hill Road, Palo Alto, CA 94304, USA

Phone: 650-812-4228 ; **FAX:** 650-812-4471 ; **E-mail:** crypto2000@iacr.org

Stipends: A limited number of stipends are available to those unable to obtain funding to attend the conference. Students whose papers are accepted and who will present the paper themselves are encouraged to apply if such assistance is needed. Requests for stipends should be addressed to the General Chair.