CRYPTO '99

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

Call For Papers

Original papers on all technical aspects of cryptology are solicited for submission to Crypto '99, the Nineteenth Annual IACR Crypto Conference. Crypto '99 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. For more information, access http://www.iacr.org/

Instructions for Authors: Authors are strongly encouraged to submit their papers electronically. A detailed description of the electronic submission procedure will appear by December 1, 1998 at
http://www.iacr.org/conferences/c99/submit.html
Electronic submissions must conform to this procedure and be received by February 8, 1999, 17:00 EST in order to be considered. Authors unable to submit electronically are invited to send a cover letter and 22 copies of an anonymous paper (double-sided copies preferred) to the Program Chair at the postal address below. Submissions must be received by the Program Chair on or before February 8, 1999 (or postmarked by January 31, 1999, 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.

Submissions must not substantially duplicate work that any of the authors have published elsewhere or have submitted in parallel to any other conference or workshop that has proceedings. 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 key words, and its introduction should summarize the contributions of the paper at a level appropriate for a non-specialist reader. The paper should be at most 12 pages excluding the bibliography and clearly marked appendices, and at most 20 pages in total, using at least 11-point font and reasonable margins. 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. Notification of acceptance or rejection will be sent to authors by April 22, 1999. 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 28, 1999.

Submission: February 8, 1999
Acceptance: April 22, 1999
Proceedings Version: May 28, 1999

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
Michael Wiener (chair), Entrust Technologies, Canada
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

Address for Non-Electronic Submissions:
Michael Wiener, Program Chair, Crypto '99
Entrust Technologies
750 Heron Road
Ottawa, Ontario
Canada K1V 1A7
Phone: (1) 613-247-3185 Fax: (1) 613-247-3690
E-mail: wiener@entrust.com

For Other Information Contact:
Donald Beaver, General Chair, Crypto '99
Transarc Corp.
707 Grant St.
Pittsburgh, PA 15219 USA
Phone: (1) 412-338-4365 Fax: (1) 412-338-4404
E-mail: crypto99@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.