CRYPTO '98

August 23-27, 1998, Santa Barbara, California, USA

CALL FOR PAPERS

General Information: Original papers on all technical aspects of cryptology are solicited for submission to Crypto '98, the Eighteenth Annual IACR Crypto Conference. Crypto '98 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, 1997 at

`http://www.iacr.org/conferences/c98/submit.html`

Electronic submissions must conform to this procedure 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 16, 1998 (or postmarked by February 7, 1998, 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.

Only original research contributions will be considered. 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, so 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 30, 1998. 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 June 5, 1998.

Submission: February 16, 1998 **Acceptance:** April 30, 1998 **Proceedings version:** June 5, 1998

Program Committee:

Dan Boneh *(Stanford University, USA)*
Yair Frankel *(CertCo, USA)*
Johan Håstad *(Royal Institute of Technology, Sweden)*
Hugo Krawczyk, chair *(Technion, Israel and IBM, USA)*
Alfred Menezes *(Auburn University, USA)*
Rafail Ostrovsky *(Bellcore, USA)*
Tal Rabin *(IBM Research, USA)*
Phillip Rogaway *(University of California at Davis, USA)*
Kazue Sako *(NEC, Japan)*
Don Coppersmith *(IBM Research, USA)*
Matt Franklin *(AT&T Labs - Research, USA)*
Lars Knudsen *(University of Bergen, Norway)*
Ueli Maurer *(ETH Zurich, Switzerland)*
Andrew Odlyzko *(AT&T Labs - Research, USA)*
Jean-Jacques Quisquater *(Université de Louvain, Belgium)*
Matt Robshaw *(RSA Laboratories, USA)*
Rainer Rueppel *(R^3 Security Engineering AG, Switzerland)*
Dan Simon *(Microsoft Research, USA)*
Moti Yung *(CertCo, USA)*

Advisory Members:

Burt Kaliski, chair Crypto'97 *(RSA Laboratories, USA)*
Michael J. Wiener, chair Crypto'99 *(Entrust Technologies, Canada)*
Joe Kilian, electronic submissions *(NEC Research Institute, USA)*

Address for non-electronic submissions:
Hugo Krawczyk, Program Chair, Crypto '98
Department of Electrical Engineering
Technion - Israel Institute of Technology
Technion City, Haifa 32000
ISRAEL
Phone: (972) 4-829-4652 Fax: (972) 4-832-3041
E-mail: `crypto98@ee.technion.ac.il`

For other information contact:
Andrew Klapper, General Chair, Crypto '98
Department of Computer Science
763h Anderson Hall
University of Kentucky
Lexington, KY 40506 USA
Phone: (1) 606-257-3961 Fax: (1) 606-323-1971
E-mail: `crypto98@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.