EUROCRYPT 2000

May 14–18, 2000, Bruges, BELGIUM

CALL FOR PAPERS

General Information: Original papers on all technical aspects of cryptology are solicited for submission to Eurocrypt 2000, the 19th Annual Eurocrypt Conference. Eurocrypt 2000 is organized by the International Association for Cryptologic Research (IACR). 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 September 15, 1999 at the Eurocrypt 2000 web pages (see URL below). Electronic submissions must conform to this procedure and be received by November 3, 1999, 17:00 MET in order to be considered. Authors unable to submit electronically are invited to send a cover letter and 20 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 November 3, 1999 (or postmarked by October 26, 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 has published elsewhere or has submitted in parallel to any other conference or workshop with 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 January 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 March 1, 2000.

Submission: November 3, 1999 **Acceptance:** January 26, 2000 **Proceedings version:** March 1, 2000

Program Committee:

Simon Blackburn *(Royal Holloway Univ. of London, UK)*
Dan Boneh *(Stanford Univ., USA)*
Christian Cachin *(IBM Research, Switzerland)*
Don Coppersmith *(IBM Research, USA)*
Ronald Cramer *(ETH Zürich, Switzerland)*
Hans Dobbertin *(BSI, Germany)*
Markus Jakobsson *(Bell Laboratories, USA)*
Thomas Johansson *(Lund Univ., Sweden)*
Joe Kilian *(NEC Research Institute, USA)*
Lars Knudsen *(Univ. of Bergen, Norway)*
Mitsuru Matsui *(Mitsubishi, Japan)*
Alfred Menezes *(Univ. of Waterloo, Canada)*
Moni Naor *(Weizmann Institute of Science, Israel)*
Kaisa Nyberg *(Nokia Research Center, Finland)*
Paul van Oorschot *(Entrust Technologies, Canada)*
Torben Pedersen *(Cryptomathic, Denmark)*
David Pointcheval *(ENS, France)*
Bart Preneel (chair) *(K.U.Leuven, Belgium)*
Moti Yung *(Certco, USA)*

Address for non-electronic submissions:

Bart Preneel, Program Chair Eurocrypt 2000
Katholieke Universiteit Leuven
Dept. Electrical Engineering-ESAT
Kard. Mercierlaan 94,
B-3001 Leuven, BELGIUM
Phone: +32-16-32-11-48
Fax: +32-16-32-19-86
`E-mail: bart.preneel@esat.kuleuven.ac.be`

For other information contact:

Joos Vandewalle, General Chair Eurocrypt 2000
Katholieke Universiteit Leuven
Dept. Electrical Engineering-ESAT
Kard. Mercierlaan 94,
B-3001 Leuven, BELGIUM
Phone: +32-16-32-10-50
Fax: +32-16-32-19-69
`E-mail: eurocrypt2000@esat.kuleuven.ac.be`

`http://www.esat.kuleuven.ac.be/cosic/eurocrypt2000`

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.