EUROCRYPT 2005

May 22–26, 2005, Aarhus, Denmark

CALL FOR PAPERS

General Information. Original papers on all technical aspects of cryptology are solicited for submission to Eurocrypt 2005, the 24th Annual Eurocrypt Conference. Eurocrypt 2005 is organized by the International Association for Cryptologic Research (IACR). For more information see `www.iacr.org` and `www.brics.dk/eurocrypt05/`.

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 with proceedings. Accepted submissions may not appear in 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 *including* title page and abstract, but excluding the bibliography and clearly marked appendices, and at most 24 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.

Papers must be submitted electronically. A detailed description of the electronic submission procedure will be available by September 20, 2004 at `http://www.ins.cwi.nl/eurocrypt05/`. Submissions must conform to this procedure and be received by **November 15, 2004, 18:00 Central European Time** to be considered. Late submissions and non-electronic submissions will not be considered. Authors unable to submit electronically should contact the Program Chair at the address below by October 1, 2004.

Notification of acceptance or rejection will be sent to authors by January 31, 2005. 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. Instructions about the preparation of a final proceedings version will be sent to the authors of accepted papers. The final version of the accepted papers will be due on February 28, 2005.

Submission: November 15, 2004 **Notification:** January 31, 2005 **Final Version:** February 28, 2005

Program Committee

Michael Backes *(IBM Zurich Research Laboratory)*
Daniel Bleichenbacher *(Lucent Bell Labs)*
Don Beaver *(Syntechnica, LLC)*
Ronald Cramer (chair) *(CWI & Leiden University)*
Don Coppersmith *(IBM T. J. Watson Research Center)*
Hans Dobbertin *(University of Bochum)*
Yevgeniy Dodis *(New York University)*
Marc Fischlin *(ETH Zürich)*
Steven Galbraith *(Royal Holloway,University of London)*
Shafi Goldwasser *(MIT & Weizmann Institute of Science)*
Shai Halevi *(IBM T. J. Watson Research Center)*
Johan Håstad *(Royal Institute of Technology)*
Marc Joye *(Gemplus)*
Aggelos Kiayias *(University of Connecticut)*
Eyal Kushilevitz *(Technion)*
Arjen Lenstra *(Lucent Bell Labs & TU Eindhoven)*
Phong Nguyen *(CNRS/École normale supérieure)*
Kaisa Nyberg *(Nokia)*
Tatsuaki Okamoto *(NTT)*
Rafail Ostrovsky *(U. C. L. A.)*
Carles Padró *(Universitat Politècnica de Catalunya)*
Benny Pinkas *(Hewlett-Packard Labs)*
Bart Preneel *(Katholieke Universiteit Leuven)*
Louis Salvail *(University of Aarhus)*
Palash Sarkar *(Indian Statistical Institute)*
Berry Schoenmakers *(TU Eindhoven)*
Igor Shparlinski *(Macquarie University)*
Douglas Stinson *(University of Waterloo)*
Salil Vadhan *(Harvard University)*
Moti Yung *(Columbia University)*

Program Chair
Ronald Cramer
CWI
Kruislaan 413
P. O. Box 94079
1090 GB Amsterdam
The Netherlands.
email: `cramer@cwi.nl`

General Chair
Ivan Damgård
Computer Science Department
University of Aarhus
IT-parken, Aabogade 34
DK-8200 Aarhus N
Denmark.
email: `ivan@daimi.au.dk`

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 before April 1, 2005.