EUROCRYPT 2004

May 2–6, 2004, Interlaken, Switzerland

www.zurich.ibm.com/eurocrypt2004

CALL FOR PAPERS

General Information. Original papers on all technical aspects of cryptology are solicited for submission to Eurocrypt 2004, the 23rd Annual Eurocrypt Conference. Eurocrypt 2004 is organized by the International Association for Cryptologic Research (IACR), in cooperation with the IBM Zurich Research Laboratory.

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. 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 25 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 15, 2003 at `http://www.zurich.ibm.com/eurocrypt2004`. Submissions must conform to this procedure and be received by **November 3, 2003, 23:59 UTC** to be considered. Late submissions and non-electronic submissions will not be considered. Authors unable to submit electronically should contact the conference chairs at the address below by October 1, 2003.

Notification of acceptance or rejection will be sent to authors by January 26, 2004. 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, 2004.

Submission: November 3, 2003; **Acceptance:** January 26, 2004; **Camera Ready:** March 1, 2004

Program Committee

Alex Biryukov *(Katholieke Universiteit Leuven)*
John Black *(University of Colorado at Boulder)*
Christian Cachin *(IBM Research)*
Jan Camenisch *(IBM Research)*
Jean-Sebastien Coron *(Gemplus Card International)*
Claude Crépeau *(McGill University)*
Ivan Damgård *(Aarhus University)*
Juan Garay *(Bell Labs - Lucent Technologies)*
Rosario Gennaro *(IBM Research)*
Alain Hiltgen *(UBS)*
Thomas Johansson *(Lund University)*
Antoine Joux *(DCSSI Crypto Lab)*
Joe Kilian *(NEC Laboratories America)*
Arjen Lenstra *(Citibank & Techn. Univ. Eindhoven)*
Yehuda Lindell *(IBM Research)*
Anna Lysyanskaya *(Brown University)*
Tsutomu Matsumoto *(Yokohama National Univ.)*
Daniele Micciancio *(UC San Diego)*
Omer Reingold *(AT&T Research and IAS)*
Vincent Rijmen *(Cryptomathic and IAIK)*
Phillip Rogaway *(UC Davis & Chiang Mai Univ.)*
Igor Shparlinski *(Macquarie University)*
Edlyn Teske *(University of Waterloo)*
Rebecca Wright *(Stevens Institute of Technology)*

Program and General Chairs

Christian Cachin and Jan Camenisch
IBM Research
Säumerstrasse 4
CH-8803 Rüschlikon
Switzerland
email: `eurocrypt2004@zurich.ibm.com`

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 `eurocrypt2004@zurich.ibm.com`.