Call for Papers

Eurocrypt 2007

May 20-24, 2007, Barcelona, Spain

`http://www.iacr.org/conferences/eurocrypt2007/`

Submission: November 7, 2006 **Notification:** February 7, 2007 **Final Version:** March 7, 2007

General Information

Original papers on all technical aspects of cryptology are solicited for submission to Eurocrypt 2007, the 26th Annual Eurocrypt Conference. Eurocrypt 2007 is organized by the International Association for Cryptologic Research (IACR). For more information see `http://www.iacr.org`.

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. IACR reserves the right to share information about submissions with other Program Committees. Accepted submissions may not appear in any other conference or workshop that has proceedings.

Submission Format:

- Anonymity: the submission is not required to be anonymous, but authors may choose to anonymize their paper.
- The length of the submission should be at most 12 pages excluding bibliography and appendices. It should be in single column format, use at least 11-point fonts, and have reasonable margins.
- The submission should begin with a title, a short abstract, and a list of keywords. The introduction should summarize the contributions of the paper at a level appropriate for a non-specialist reader. Committee members are not expected to read appendices; the paper should be intelligible without them.
- Papers must be submitted electronically by Nov 7, 2006, 19:00 UTC. Late submissions and non-electronic submissions (including faxes) will not be considered.
- Submissions should preferably be in PDF format, although PostScript will be allowed. If at all possible, the submission should be in US letter paper size (rather than A4), and should use Type 1 fonts (rather than Type 3 fonts). Please see the conference web page for instructions and tips on preparing your submission file.

Notification of acceptance or rejection will be sent to authors by February 7, 2007. Authors of accepted papers must guarantee that their paper will be presented at the conference.

Conference Proceedings

Proceedings will be published in Springer'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 versions of the accepted papers will be due on March 7, 2006.

Important Dates

Submission: November 7, 2006 **Notification:** February 7, 2007 **Final Version:** March 7, 2007

Program Committee

Michel Abdalla (ENS)
Anne Canteaut (INRIA-Rocquencourt)
Dario Catalano (Univ. of Catania)
Jung Hee Cheon (Seoul National Univ.)
Stefan Dziembowski (Warsaw Univ. & Univ. of Rome 1)
Serge Fehr (CWI)
Marc Fischlin (TU Darmstadt)
Jens Groth (UCLA)
Shai Halevi (IBM Watson Research Center)
Yuval Ishai (Technion)
Joe Kilian (Rutgers Univ.)
Anna Lysyanskaya (Brown Univ.)
Alexander May (TU Darmstadt)
Steven Myers (Univ. of Indiana)
Moni Naor **(chair)** (Weizmann Inst. of Sci.)
Phong Nguyen (CNRS/ENS, Paris)
Jesper Buus Nielsen (Aarhus Univ.)
Giuseppe Persiano (Univ. of Salerno)
Ron Rivest (MIT)
Alon Rosen (Harvard)
Eran Tromer (MIT)
Brent Waters (SRI)
Xiaoyun Wang (Tsinghua Univ.)
Stefan Wolf (ETH Zurich)

Advisory members: Nigel Smart (Univ. of Bristol) Serge Vaudenay (EPFL)

Conference chairs

Program Chair:

Moni Naor
Dept. Computer Science and Applied Mathematics
Weizmann Institute of Science
Rehovot 76100
ISRAEL
Email: `eurocrypt07_program_chair(at)weizmann.ac.il`

General Chairs:

Javier López
Computer Science Department
E.T.S. Ingeniera Informática
Campus de Teatinos
University of Málaga
29071 Málaga
SPAIN
Tel: +34-952-131327
Fax: +34-952-131327 (same as phone)
Email: `eurocrypt2007(at)iacr.org`

Germán Sáez
Department of Applied Mathematics IV
E.T.S. Enginyeria de Telecomunicació de Barcelona
Campus Nord
Universitat Politècnica de Catalunya
08034 Barcelona
SPAIN
Tel: +34-93-4016002
Fax: +34-93-4015981
Email: `eurocrypt2007(at)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 `stipends_ec07@ma4.upc.edu` before April 1, 2007.