EUROCRYPT 2010

Nice, French Riviera, France

May 30–June 3, 2010

Call for Papers

Original papers on all technical aspects of cryptology are solicited for submission to Eurocrypt 2010, the 29th annual Eurocrypt conference. Eurocrypt 2010 is organized by the International Association for Cryptologic Research (IACR), `http://www.iacr.org/`.
The conference homepage is `http://crypto.rd.francetelecom.com/events/eurocrypt2010/`.

Important Dates

submission deadline:
October 20, 2009 23:59 UTC

notification to authors:
January 29, 2010

proceedings version deadline:
February 26, 2010

Conference Organization

All correspondence and/or questions should be directed to either of the organizational committee members:

Henri Gilbert
Program Chair
Orange Labs / MAPS / STT
38-40 rue du Général Leclerc
92794 Issy les Moulineaux Cedex 9, France
henri.gilbert@orange-ftgroup.com
phone: +33 1 4529 5497

Olivier Billet and Matt Robshaw
General Chairs
Orange Labs / MAPS / STT
38-40 rue du Général Leclerc
92794 Issy les Moulineaux Cedex 9, France
eurocrypt2010@iacr.org
phone: +33 1 4529 6783

Program Committee

Dan Boneh *Stanford University*
Ran Canetti *Tel Aviv University*
Anne Canteaut *INRIA*
Carlos Cid *Royal Holloway, University of London*
Jean-Sébastien Coron *Université du Luxembourg*
Ivan Bjerre Damgård *University of Aarhus*
Steven Galbraith *Auckland University*
Rosario Gennaro *IBM Research*
Henri Gilbert *Orange Labs*
Helena Handschuh *K.U.Leuven and Intrinsic-ID Inc.*
Stanislaw Jarecki *University of California at Irvine*
Antoine Joux *DGA and Université de Versailles*
Marc Joye *Thomson R&D*
Ari Juels *RSA Laboratories*
Aggelos Kiayias *University of Connecticut*
Lars R. Knudsen *Technical University of Denmark*
Arjen K. Lenstra *EPFL and Alcatel-Lucent Bell Laboratories*
Helger Lipmaa *Cybernetica AS*
Mitsuru Matsui *Mitsubishi Electric*
Alexander May *Ruhr-University Bochum*
Tatsuaki Okamoto *NTT*
Krzysztof Pietrzak *CWI Amsterdam*
David Pointcheval *ENS/CNRS/INRIA*
Bart Preneel *Katholieke Universiteit Leuven*
Phillip Rogaway *University of California, Davis*
Amit Sahai *UCLA*
Berry Schoenmakers *Technische Universiteit Eindhoven*
Ron Steinfeld *Macquarie University*
Frederik Vercauteren *Katholieke Universiteit Leuven*
Yiqun Lisa Yin *Independent Security Consultant*

Instructions for Authors

The submission must be anonymous with no author names, affiliations or obvious references. The length of the submission must be at most 14 pages excluding references and appendices. The text should be in a single column format, in at least 11-point fonts and have reasonable margins. If the submission is accepted, the length of the final version for Springer's LNCS will be at most 20 pages including references and appendices. 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 the level understandable for a non-expert reader. The reviewers 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.

Submissions must not substantially duplicate work that any of the authors has published in a journal or a conference/workshop with proceedings, or has submitted/is planning to submit before the author notification deadline to a journal or other conferences/workshops that have proceedings. Accepted submissions may not appear in any other conference or workshop that has proceedings. IACR reserves the right to share information about submissions with other program committees to detect parallel submissions and the IACR policy on irregular submissions will be strictly enforced. For further details, see `http://www.iacr.org/irregular.html`. Program committee members are restricted to one submission each.

It is encouraged that the submission be processed in LaTeX2e according to the instructions listed on `http://www.springer.de/comp/lncs/authors.html`. These instructions are mandatory for the final papers. Submitted papers must be in PDF format and should be submitted electronically. A detailed description of the electronic submission procedure will be announced at the conference homepage.

Notification of acceptance or rejection will be sent to authors by January 29, 2010.

Conference Proceedings

Proceedings will be published in Springer's Lecture Notes in Computer Science and will be available at the conference. Authors of accepted papers must complete the IACR copyright assignment form at `http://www.iacr.org/forms/copyright_agreement.html` for their work to be published in the proceedings, and guarantee that their paper will be presented at the conference. The final versions of the accepted papers will be due on February 26, 2010.

Stipends

Students presenting their papers at the conference will have their registration fee waived. In addition, a limited number of stipends are available to students who are unable to get funding to attend the conference. Requests for registration waiver or stipends should be addressed to the general chairs.