Call for Papers
CRYPTO 2011
August 14–18, 2011
Santa Barbara, California, USA
www.iacr.org/conferences/crypto2011/

Submission deadline Feb 17, 2011 at 23:59 UTC (3:59 pm PST)
Notification Apr 29, 2011
Proceedings version due May 27, 2011

General Information

Original papers on all technical aspects of cryptology are solicited for submission to CRYPTO 2011, the 31st Annual International Cryptology Conference. Besides the usual topics, submissions are also welcome on topics not routinely appearing at recent CRYPTOs, including cryptographic work in the style of the CHES workshop or CSF symposium. CRYPTO 2011 is sponsored by the International Association for Cryptologic Research (IACR), in cooperation with the Computer Science Department of the University of California, Santa Barbara.

Instructions for Authors

Submissions must be anonymous with no author names, affiliations, or obvious references. Submissions must be at most 12 pages, excluding references and appendices. The paper must be in single-column format, use at least 11-point fonts, and have reasonable margins. Submissions should begin with a title, a short abstract, and a list of keywords. The introduction should summarize the paper’s contributions at a level understandable to a non-expert in the field. Reviewers are not required to read appendices, so papers should be intelligible without them.

Submissions should be prepared using LaTeX and submitted as PDF using type-1 fonts. Papers must be submitted electronically; a detailed description of the electronic submission procedure will be provided on the conference homepage, http://www.iacr.org/conferences/crypto2010/

Submissions must not substantially duplicate work that any of the authors published, submitted, or is planning to submit before the notification-date to any conference/workshop with proceedings. Accepted submissions may not appear in any other conference or workshop that has proceedings. The program committee may share information about submitted papers with other conference chairs to ensure adherence to this policy. Authors uncertain whether their submission meets the IACR rules should contact the program chair. The authors of submitted papers guarantee that their paper will be presented at the conference if it is accepted. Submissions not meeting any of the guidelines above risk rejection without consideration of their merits.

Proceedings

Proceedings will be published in Springer’s Lecture Notes in Computer Science series, and will be available at the conference. Instructions for the preparation of the proceedings version will be sent to the authors of accepted papers. Authors will need to provide a signed IACR Copyright form along with the proceedings version of their papers.
Program Chair
Phillip Rogaway
Dept. of Computer Science
One Shields Ave.
University of California
Davis, California 95616 USA
phone +1 530 752 7583
rogaway@cs.ucdavis.edu

General Chair
Tom Shrimpton
Dept. of Computer Science
PO Box 751
Portland State University
Portland, Oregon 97201 USA
+1 503 725 4055
teshrim@cs.pdx.edu

Advisory Members
Tal Rabin
CRYPTO 2010
Program Chair
Rei Safavi-Naini
CRYPTO 2012
Program Chair

Program Committee
Masayuki Abe
NTT, Japan
Michael Backes
Saarland University and MPI-SWS, Germany
Paulo Barreto
University of São Paulo, Brazil
Mihir Bellare
UC San Diego, USA
Alex Biryukov
University of Luxembourg
Dan Boneh
Stanford, USA
Jung Hee Cheon
Seoul National University, Korea
Jean-Sébastien Coron
University of Luxembourg
Marten van Dijk
RSA Labs and MIT/CSAIL, USA
Yevgeniy Dodis
New York University, USA
Orr Dunkelman
Weizmann Institute, Israel
Serge Fehr
CWI, The Netherlands
Steven Galbraith
University of Auckland, New Zealand
Craig Gentry
IBM Watson, USA
Louis Goubin
Université de Versailles, France
Vipul Goyal
Microsoft Research, India
Aggelos Kiayias
University of Connecticut, USA
Elke Kiltz
Universität Bochum, Germany
Anja Lehmann
IBM Zurich, Switzerland
Arjen Lenstra
EPFL, Switzerland
Stefan Mangard
Infineon Technologies, Germany
Daniele Micciancio
UC San Diego, USA
Tal Moran
Harvard, USA
Chanathip Namprempre
Thammasat University, Thailand
Phong Nguyen
INRIA and ENS, France
Jesper Buus Nielsen
Århus University, Denmark
Rafael Pass
Cornell University, USA
Kenny Paterson
Royal Holloway, University of London, UK
Benny Pinkas
Bar Ilan University, Israel
Bart Preneel
Katholieke Universiteit Leuven, Belgium
Leonid Reyzin
Boston University, USA
Vincent Rijmen
K.U. Leuven, Belgium & TU Graz, Austria
Phillip Rogaway
UC Davis, USA (Program Chair)
Rei Safavi-Naini
U. of Calgary, Canada (Junior Program Chair)
Andre Scedrov
University of Pennsylvania, USA
Adam Smith
Pennsylvania State University, USA
François-Xavier Standaert
UCL, Belgium
Stefano Tessaro
UC San Diego, USA
Bogdan Warinschi
University of Bristol, UK
Hoeteck Wee
Queens College, CUNY, USA

Stipends
A limited number of stipends are available to those unable to obtain funding to attend the conference, and to students having an accepted paper that they will present. Requests for stipends should be addressed to the general chair.