CRYPTO 2014 | Call for Papers

The 34th Annual International Cryptology Conference

August 17-21, 2014, Santa Barbara, CA

http://www.iacr.org/conferences/crypto2014/

General Information

Original contributions on all technical aspects of cryptology are solicited for submission to CRYPTO 2014, the 34th Annual International Cryptology Conference. This includes works on foundational, applied, and industry-related aspects of the discipline. Innovative, "outside the box" papers are particularly solicited. CRYPTO 2014 is sponsored by the International Association for Cryptologic Research (IACR), in cooperation with the Computer Science Department of the University of California, Santa Barbara.

Important Dates

Submission deadline:	February 10, 2014 at 22:00 UTC (5:00 pm EST)
First round of comments:	April 14, 2014
Responses to comments due:	April 17, 2014 at 22:00 UTC (6:00 pm EDT)
Notification of decision:	May 19, 2014
Proceedings version due:	June 13, 2014
Conference:	August 17-21, 2014

Instructions for Authors

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 must be presented in a way that allows the understanding and verification of the claimed results with reasonable time and effort.

Submissions must be anonymous, with no author names, affiliations, or obvious references. It is recognized that, at times, information regarding the identities of authors may become public outside the paper submission process. The PC will ignore this external information.

Submissions should be prepared using LaTeX and submitted in PDF format using type-1 fonts (see this page for help). Papers must be submitted electronically; a detailed description of the electronic submission procedure will be provided on the conference homepage.

Submissions must not substantially duplicate work that any of the authors published, submitted, or are planning to submit before the notification date to any journal or 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 conforms to IACR policy should contact the program chairs. The authors of submitted papers guarantee that their paper will be presented at the conference by one of the authors if it is accepted.

Submissions not meeting any of the guidelines above risk rejection without consideration of their merits.

Best Young Researcher Paper Award

In a continuing effort to promote independent work by young researchers, this year we again plan to have in addition to the general best paper award, a prize for the best paper that is authored exclusively by young researchers. To be eligible, all co-authors must be either full-time students or have received their PhD degree in 2012 or later. As usual, awards will be given only if deserving papers are identified.

Interim Reviews and Rebuttal

Authors will be given the opportunity to comment on the initial reviews written on their submissions. Commenting is optional; it is not a requirement. The dates are listed above. Additional details regarding the format and exact procedure will be available at the conference homepage.

Proceedings

Proceedings will be published in Springer's *Lecture Notes in Computer Science* series, and will be available at the conference, either physically or electronically. 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.

Stipends

A limited number of stipends will be 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.

Contact Information

General Chair:

Alexandra Boldyreva
Klaus Advanced Computing
Georgia Institute of Technology
266 Ferst Dr.
Atlanta, GA 30332-0765, USA
Tel: +1 404 385 6753
Email: crypto2014@iacr.org

Program Co-Chairs:

Juan A. Garay
Yahoo Labs
701 First Ave.
Sunnyvale, CA 94089, USA

Rosario Gennaro
The City College of New York
160 Convent Avenue
New York, NY 10031, USA

Email: crypto2014programchairs@iacr.org

Advisory Member

Ran Canetti
Boston U., USA and Tel-Aviv U., Israel
CRYPTO 2013 Program Co-Chair

Program Committee

Yevgeniy Dodis	NYU, USA
Orr Dunkelman	U. of Haifa, Israel
Serge Fehr	CWI, The Netherlands
Pierre-Alain Fouque	U. Rennes 1, France
Craig Gentry	IBM Research, USA
Vipul Goyal	MSR, India
Nadia Heninger	U. of Pennsylvania, USA
Thomas Holenstein	ETH, Switzerland
Yuval Ishai	Technion, Israel
Dimitar Jetchev	EPFL, Switzerland
Aggelos Kiayias	U. of Athens, Greece
Kaoru Kurosawa	Ibaraki U., Japan
Alexander May	U. Bochum, Germany
Ilya Mironov	MSR, USA
Payman Mohassel	U. of Calgary, Canada
Jörn Müller-Quade	KIT, Germany
María Naya-Plasencia	INRIA, France
Claudio Orlandi	Aarhus U., Denmark
Rafael Pass	Cornell U., USA
Chris Peikert	Georgia Tech, USA
Krzysztof Pietrzak	IST Austria
Leo Reyzin	Boston U., USA
Ron Rivest	MIT, USA
Amit Sahai	UCLA, USA
Gil Segev	Hebrew U., Israel
Elaine Shi	U. of Maryland, USA
Tom Shrimpton	Portland State U., USA
Alice Silverberg	UC Irvine, USA
Marc Stevens	CWI, The Netherlands
Katsuyuki Takashima	Mitsubishi Electric, Japan
Stefano Tessaro	UCSB, USA
Vinod Vaikuntanathan	MIT, USA
Gilles Van Assche	STM, Belgium
M.Venkitasubramaniam	U. of Rochester, USA
Ivan Visconti	U. of Salerno, Italy
Bogdan Warinschi	U. of Bristol, UK
Brent Waters	UT Austin, USA
Vassilis Zikas	UCLA, USA