Call for Papers CRYPTO 2012

August 19–23, 2012
Santa Barbara, California, USA

www.iacr.org/conferences/crypto2012/

Submission deadline	Feb 17, 2012 at **23:59 UTC** (3:59 pm PST)
Notification	**Apr 30, 2012**
Proceedings version due	**June 1, 2012**

General Information

Original papers on all technical aspects of cryptology are solicited for submission to CRYPTO 2012, the 32nd Annual International Cryptology Conference. This includes works on foundational, and application and implementation oriented topics. New cryptographic models and solutions to real-world problems, and innovative "out of the box" papers are particularly solicited. CRYPTO 2012 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 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, sometimes, information regarding the identities of authors inevitably becomes public outside the paper submission. The PC will ignore this external information.

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/crypto2012/

Submissions must not substantially duplicate work that any of the authors published, submitted, or is 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 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

Rei Safavi-Naini
University of Calgary

Program co-Chair

Ran Canetti
Boston Univ. & Tel Aviv Univ.

General Chair

Yiqun Lisa Yin
Independent Security Consultant

Advisory Member

Phil Rogaway
CRYPTO 2011
Program Chair

Program Committee

Benny Applebaum	Tel-Aviv University, Israel
Dan Boneh	Stanford, USA
Colin Boyd	QUT, Australia
Ran Canetti	Boston Univ.& Tel Aviv Univ., USA&Israel
Ivan Damgård	Aarhus University, Denmark
Yevgeniy Dodis	New York University, USA
Serge Fehr	CWI Amsterdam, The Netherlands
Cédric Fournet	Microsoft Research, UK
Marc Fischlin	Darmstadt University of Technology, Germany
Pierre-Alain Fouque	École Normale Supérieure, France
Juan Garay	AT&T Labs - Research, USA
Steven Galbraith	The University of Auckland, New Zealand
Jens Groth	University College London, UK
Susan Hohenberger	Johns Hopkins University, USA
Yuval Ishai	Technion, Israel
Ari Juels	RSA Laboratories, USA
Yael Kalai	Microsoft Research, USA
Hugo Krawczyk	IBM Research, USA
Ralf Küsters	University of Trier, Germany
Aggelos Kiayias	University of Connecticut, USA
Kaoru Kurosawa	Ibaraki University, Japan
Stefan Lucks	Bauhaus-Universität Weimar, Germany
Tal Malkin	Columbia University, USA
Alexander May	Ruhr-University Bochum, Germany
Daniele Micciancio	University of California at San Diego, USA
Kaisa Nyberg	Aalto University and Nokia, Finland
Tatsuaki Okamoto	NTT, Japan
Kenny Paterson	Royal Holloway, University of London, UK
Chris Peikert	Georgia Tech, USA
Thomas Peyrin	Nanyang Technological University, Singapore
Bart Preneel	KU Leuven, Belbium
Renato Renner	ETH Zurich, Switzerland
Rei Safavi-Naini	University of Calgary, Canada
Palash Sarkar	Indian Statistical Institute, Kolkata, India
François-Xavier Standaert	UCL, Belgium
Damien Stehlé	CNRS and ENS de Lyon, France
Thomas Shrimpton	Portland State University, USA
Tsuyoshi Takagi	Kyushu University, Japan
Eran Tromer	Tel Aviv University, Israel
Dominique Unruh	University of Tartu, Estonia
Vinod Vaikuntanathan	University of Toronto, Canada

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.