Call for Papers: CRYPTO 2013

Important Dates

Submission deadline:	February 15, 2013 at 22:00 UTC (5:00 pm EST)
First round of comments:	April 1, 2013
Responses to comments due:	April 4, 2013 at 22:00 UTC (5:00 pm EST)
Notification of decision:	May 6, 2013
Proceedings version due:	June 8, 2013
Conference:	August 18-22, 2013

General Information

Original papers on all technical aspects of cryptology are solicited for submission to CRYPTO 2013, the 33rd Annual International Cryptology Conference. This includes works on foundational, practical, and industry related aspects. Innovative, ``outside the box'' papers are particularly solicited. CRYPTO 2013 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 anonymized with no author names, affiliations, or obvious references. It is recognized that, sometimes, 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 as PDF 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 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 conforms to IACR policy 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 these guidelines risk rejection without consideration of their merits.

Best Young Researcher Paper Award

In an effort to promote independent work by young researchers, this year we plan to have in addition to the general best paper award, also 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 2011 or later. As usual, awards will be given only if deserving papers are identified.

Interim reviews and rebuttal

This year 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 are available here.

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 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. Additional details are available here.

Program Committee

Masayuki Abe	*NTT, Japan*
Mihir Bellare	*UCSD, USA*
Zvika Brakerski	*Stanford, USA*
Jan Camenisch	*IBM Research, Zurich, Switzerland*
Ran Canetti	*BU, USA and TAU, Israel (co-chair)*
David Cash	*Rutgers, USA*
Kai-Min Chung	*Cornell, USA and Academia Sinica, Taiwan*
Jean-Sebastien Coron	*U. Luxemburg*
Dana Dachman-Soled	*Microsoft Research, USA*
Stefan Dziembowski	*U. Warsaw, Poland and U. Rome I, Italy*
Juan Garay	*AT&T, USA (co-chair)*
Iftach Haitner	*TAU, Israel*
Shai Halevi	*IBM Research, USA*
Goichiro Hanaoka	*AIST, Japan*
Dennis Hofheinz	*KIT, Germany*
Jonathan Katz	*U. Maryland, USA*
Lars R. Knudsen	*DTU, Denmark*
Eyal Kushilevitz	*Technion, Israel*
Kristin Lauter	*Microsoft Research, USA*
Huijia Rachel Lin	*MIT & BU, USA*
Yehuda Lindell	*BIU, Israel*
Vadim Lyubashevsky	*ENS, France*
John Mitchell	*Stanford, USA*
Tal Moran	*IDC, Israel*
Jesper Buus Nielsen	*U. Aarhus, Denmark*
Christof Paar	*U. Bochum, Germany*
Manoj Prabhakaran	*UIUC, USA*
Tal Rabin	*IBM Research, USA*
Charlie Rackoff	*U. Toronto, Canada*
Christian Rechberger	*DTU, Denmark*
Thomas Ristenpart	*U. Wisconsin, USA*
Guy Rothblum	*Microsoft Research, USA*
Christian Schaffner	*U. Amsterdam, The Netherlands*
Vitaly Shmatikov	*UT Austin, USA*
Hovav Shacham	*UCSD, USA*
Nigel Smart	*U. Bristol, UK*
Adam Smith	*Penn State, USA*
Martijn Stam	*U. Bristol, UK*
John Steinberger	*Tsinghua, China*
Frederik Vercauteren	*KU Leuven, Belgium*
Xiaoyun Wang	*Tsinghua, China*
Daniel Wichs	*Northeastern, USA*

Advisory Member

Rei Safavi-Naini *CRYPTO 2012 Program Chair*

General Chair:

Helena Handschuh
Cryptography Research Inc. and K.U. Leuven