Crypto 2018 Call for Papers

Original contributions on all technical aspects of cryptology are solicited for submission to Crypto 2018, the 38th Annual International Cryptology Conference. Submissions are welcomed on any cryptographic topic including, but not limited to:

- foundational theory and mathematics;
- the design, proposal, and analysis of cryptographic primitives and protocols;
- secure implementation and optimization in hardware or software; and
- applied aspects of cryptography.

Crypto 2018 is sponsored by the International Association for Cryptologic Research (IACR), in co-operation with the Computer Science Department of the University of California, Santa Barbara. The proceedings of Crypto 2018 will be published by Springer in the LNCS series.

Instructions for Authors

Submissions must use the Springer LNCS format with the default margins and font, with one modification: submissions *must* display page numbers (e.g., by adding `\pagestyle{plain}` to the document preamble). Submissions may contain at most 30 pages including the title page, bibliography, and figures. Optionally, any amount of clearly marked supplementary material may be supplied, following the main body of the paper or in separate files; however, reviewers are not required to read or review any supplementary material, and submissions are expected to be intelligible and complete without it. The final published version of an accepted paper is expected to closely match the submitted 30 pages that are reviewed.

Submissions should begin with a title and abstract, followed by an introduction that summarizes the paper's contribution in a manner that is understandable to a general cryptographic audience. Submissions must be anonymous, with no author names, affiliations, or obvious references; all submissions will be blind-refereed. Submissions must not substantially duplicate published work or work that has been submitted in parallel to any other journal or conference/workshop with published proceedings. All submissions to Crypto 2018 are viewed as active submissions throughout the entire review period, and may not be submitted to any other journal or conference/workshop with published proceedings before the notification date. Accepted submissions cannot appear in any other conference or workshop that has published proceedings. The IACR reserves the right to share information about submissions with other program committees to check for violations of these rules. The conference will follow the IACR *Policy on Irregular Submissions* available at `https://www.iacr.org/docs/`; authors may wish to consult the IACR *Guidelines for Authors* available there as well.

Papers must be submitted electronically; a detailed description of the submission procedure will be available on the conference webpage. Submissions not meeting the guidelines above may be rejected without consideration of their merits. All accepted papers must conform to the Springer publishing requirements, and authors will be required to sign the IACR Copyright form when submitting the proceedings version of their paper. By submitting a paper, the authors agree that if the paper is accepted, one of the authors will present the paper at the conference and, in addition, will grant permission to the IACR to distribute the presentation slides as well as an audio/video recording of the presentation as per the IACR copyright and consent form.

- Submission deadline: **February 13, 2018, 16:00 EST**
- Reviews sent out for rebuttal: April 1, 2018
- Rebuttal deadline: April 4, 2018
- Paper notification: April 29, 2018
- Final version due: June 3, 2018
- Conference dates: August 19–23, 2018

Awards

The Program Committee may choose a paper to receive an overall best paper award. In a continuing effort to promote independent work by researchers at an early stage in their career, the Program Committee may also award a prize for the best paper authored exclusively by early-career researchers. To be eligible, all co-authors must be studying full/part-time or have received their degree in 2016 or later. As usual, awards will only be given if deserving papers are identified.

Stipends

The IACR's Cryptography Research Fund allows us to waive the registration fee for all student presenters of an accepted paper (application required). Thanks to our sponsors' generosity, a limited number of stipends will also be available to students unable to obtain funding to attend the conference. Students in under-represented groups are especially encouraged to apply. To apply, go to the stipends webpage, `https://crypto.iacr.org/2018/stipends.html`. Contact the general chair with any question.

Program Committee

Shweta Agrawal, Indian Institute of Technology, Madras
Benny Applebaum, Tel Aviv University
Foteini Baldimtsi, George Mason University
Gilles Barthe, IMDEA Software Institute
Fabrice Benhamouda, IBM Research
Alex Biryukov, University of Luxembourg
Jeremiah Blocki, Purdue University
Anne Broadbent, University of Ottawa
Chris Brzuska, Aalto University
Chitchanok Chuengsatiansup, Inria and ENS de Lyon
Dana Dachman-Soled, University of Maryland
Léo Ducas, Centrum Wiskunde & Informatica
Pooya Farshim, CNRS and ENS
Dario Fiore, IMDEA Software Institute
Marc Fischlin, Darmstadt University of Technology
Georg Fuchsbauer, Inria and ENS
Steven Galbraith, University of Auckland
Christina Garman, Purdue University
Daniel Genkin, University of Pennsylvania and University of Maryland
Dov Gordon, George Mason University
Viet Tung Hoang, Florida State University
Tetsu Iwata, Nagoya University
Stanislaw Jarecki, University of California, Irvine
Seny Kamara, Brown University
Markulf Kohlweiss, University of Edinburgh
Farinaz Koushanfar, University of California, San Diego
Xuejia Lai, Shanghai Jiao Tong University
Tancrède Lepoint, SRI International
Anna Lysyanskaya, Brown University
Alex J. Malozemoff, Galois
Sarah Meiklejohn, University College London
Daniele Micciancio, University of California, San Diego
María Naya-Plasencia, Inria
Kenny Paterson, Royal Holloway, University of London
Ananth Raghunathan, Google
Mike Rosulek, Oregon State University
Ron Rothblum, MIT and Northeastern University
Alessandra Scafuro, North Carolina State University
abhi shelat, Northeastern University
Nigel Smart, Katholieke Universiteit Leuven
Martijn Stam, University of Bristol
Noah Stephens-Davidowitz, Princeton University
Aishwarya Thiruvengadam, University of California, Santa Barbara
Hoeteck Wee, CNRS and ENS
Daniel Wichs, Northeastern University
Mark Zhandry, Princeton University

Advisory Member: Jonathan Katz, University of Maryland, Crypto 2017 Program Co-Chair

Contact Information

General Chair: Tal Rabin
IBM T.J. Watson Research Center
Yorktown Heights, NY 10598, USA
`crypto2018@iacr.org`

Program Co-Chairs: Alexandra Boldyreva
School of Computer Science
Georgia Institute of Technology
Atlanta, GA 30332, USA

Hovav Shacham
Department of Computer Science
University of Texas at Austin
Austin, TX 78712, USA

`crypto2018programchairs@iacr.org`