Crypto 2020 Call for Papers

Original contributions on all technical aspects of cryptology are solicited for submission to Crypto 2020, the 40th 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 2020 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 2020 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 without it. Significant changes between the published version and the submitted version should be approved by the program committee.

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 2020 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. When applicable, we encourage authors to include in their supplementary materials the responses to reviews from prior IACR events as described at `https://iacr.org/docs/author.pdf`. During submission, the authors will be asked to indicate any conflicts of interest with the PC members. The IACR CoI policy can be found at `https://www.iacr.org/docs/conflicts.pdf/`

- Submission deadline: **February 11, 2020, 21:00 UTC**
- Reviews sent out for rebuttal: March 27, 2020
- Rebuttal deadline: April 3, 2020
- Paper notification: May 8, 2020
- Final version due: June 15, 2020
- Conference dates: August 16–20, 2020

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 2018 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/2020/stipends.html`. Contact the general chair with any questions.

Program Committee

Daniele Micciancio, UC San Diego (program co-chair)
Thomas Ristenpart, Cornell Tech (program co-chair)
Adi Akavia, University of Haifa
Martin Albrecht, Royal Holloway University
Roberto Avanzi, ARM
Lejla Batina, Radboud University, The Netherlands
Jeremiah Blocki, Purdue University
David Cash, University of Chicago
Melissa Chase, Microsoft Research
Hao Chen, Microsoft Research
Ilaria Chillotti, KU Leuven
Henry Corrigan-Gibbs, EPFL and MIT
Craig Costello, Microsoft Research
Joan Daemen, Radboud University Nijmegen
Thomas Eisenbarth, University of Lübeck
Pooya Farshim, University of York
Sanjam Garg, University of California, Berkeley
Daniel Genkin, University of Michigan
Steven Goldfeder, Cornell Tech
Shay Gueron, University of Haifa, Israel and AWS, US
Felix Günther, ETH Zurich
Tetsu Iwata, Nagoya University
Tibor Jager, Bergische Universitaet Wuppertal
Antoine Joux, Fondation Partenariale de Sorbonne Université
Jonathan Katz, George Mason Univ
Eike Kiltz, RU Bochum
Elena Kirshanova, ENS Lyon
Venkata Koppula, Weizmann Institute of Science
Anna Lysyanskaya, Brown University
Vadim Lyubashevsky, IBM Research
Mohammad Mahmoody, University of Virginia
Florian Mendel, Infineon Technologies, Germany
María Naya-Plasencia, Inria, France
Adam O'Neill, UMass
Olya Ohrimenko, Microsoft Research
Claudio Orlandi, Aahrus University
Elisabeth Oswald, University of Klagenfurt
Chris Peikert, University of Michigan
Bertram Poettering, IBM Research
Antigoni Polychroniadou, JP Morgan
Ananth Raghunathan, Google
Mariana Raykova, Google
Christian Rechberger, TU Graz
Alon Rosen, IDC
Mike Rosulek, Oregon State University
Alessandra Scafuro, NC State
Dominique Schröder, Friedrich-Alexander-Universität Erlangen-Nürnberg
Thomas Shrimpton, University of Florida
Fang Song, Texas A&M University
Marc Stevens, CWI Amsterdam
Dominique Unruh, University of Tartu
Michael Walter, IST Vienna, Austria
David Wu, University of Virginia

Advisory Member: Alexandra Boldyreva, Georgia Institute of Technology, Crypto 2019 Program Co-Chair.

Contact Information

General Chair:
Leonid Reyzin
Boston University
Boston, MA 02215, USA
`crypto2020@iacr.org`

Program Co-Chairs:
Daniele Micciancio
Department of Computer Science
UC San Diego
La Jolla, CA 92093, USA

Thomas Ristenpart
Department of Computer Science
Cornell Tech
New York, NY 10044, USA

`crypto2020programchairs@iacr.org`