Crypto 2019 Call for Papers

Original contributions on all technical aspects of cryptology are solicited for submission to Crypto 2019, the 39th 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 2019 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 2019 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 2019 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 13, 2019, 16:00 EST**
- Reviews sent out for rebuttal: March 26, 2019
- Rebuttal deadline: March 29, 2019
- Paper notification: April 29, 2019
- Final version due: June 2, 2019
- Conference dates: August 18–22, 2019

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 2017 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/2019/stipends.html`. Contact the general chair with any question.

Program Committee

Manuel Barbosa, INESC TEC & University of Porto (FCUP)
Zvika Brakerski, Weizmann Institute of Science
Mark Bun, Simons Institute & Boston University
Ran Canetti, Boston University & Tel Aviv University
Dario Catalano, Università di Catania
Alessandro Chiesa, UC Berkeley
Sherman S. M. Chow, Chinese University of Hong Kong
Kai-Min Chung, Academia Sinica
Jean-Sébastien Coron, University of Luxembourg
Jean Paul Degabriele, TU Darmstadt
Nico Döttling, Cispa Helmholtz Center i.G.
Orr Dunkelman, University of Haifa
Rosario Gennaro, The City College of New York
Tim Güneysu, Ruhr-Universität Bochum & DFKI
Felix Günther, UC San Diego
Siyao Guo, NYU Shanghai
Sean Hallgren, Pennsylvania State University
Carmit Hazay, Bar-Ilan University
Susan Hohenberger, Johns Hopkins University
Sorina Ionica, Université de Picardie
Bhavana Kanukurthi, Indian Institute of Science
Vladimir Kolesnikov, Georgia Institute of Technology
Anja Lehmann, IBM Research - Zurich
Vadim Lyubashevsky, IBM Research - Zurich
Ilya Mironov, Google
Michael Naehrig, Microsoft Research
Svetla Nikova, KU Leuven
Ryo Nishimaki, NTT Secure Platform Laboratories
Omer Paneth, MIT
Charalampos Papamanthou, University of Maryland
Chris Peikert, University of Michigan
Giuseppe Persiano, Università di Salerno
Christophe Petit, University of Birmingham
Thomas Peyrin, Nanyang Technological University
Benny Pinkas, Bar Ilan University
Bertram Poettering, Royal Holloway, University of London
Mariana Raykova, Yale University
Silas Richelson, UC Riverside
Adeline Roux-Langlois, Univ Rennes, CNRS, IRISA
Peter Scholl, Aarhus University
Dominique Schröder, Friedrich-Alexander-Universität Erlangen-Nürnberg
Thomas Shrimpton, University of Florida
Damien Stehlé, ENS de Lyon
Björn Tackmann, IBM Research - Zurich
Keisuke Tanaka, Tokyo Institute of Technology
Eran Tromer, Tel Aviv University & Columbia University
Daniele Venturi, Sapienza University of Rome
Xiao Wang, MIT & Boston University
Xiaoyun Wang, Tsinghua University
Bogdan Warinschi, University of Bristol
Mor Weiss, IDC Herzliya

Advisory Member: Hovav Shacham, University of Texas at Austin, Crypto 2018 Program Co-Chair.

Contact Information

General Chair:
Muthuramakrishnan Venkitasubramaniam
University of Rochester,
Rochester, NY 14627, USA
`crypto2019@iacr.org`

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

Daniele Micciancio
Department of Computer Science
UC San Diego
La Jolla, CA 92093, USA

`crypto2019programchairs@iacr.org`