Crypto 2017 Call for Papers

Original contributions on all technical aspects of cryptology are solicited for submission to Crypto 2017, the 37th Annual International Cryptology Conference. Submissions are welcome on any cryptographic topics including, but not limited to:

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

Crypto 2017 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 2017 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, and 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 after 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 2017 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. Submissions not meeting the listed guidelines may be rejected without consideration of their merits.

Papers must be submitted electronically; a detailed description of the submission procedure will be available on the conference webpage. All accepted papers must conform to the Springer publishing requirements, and authors will be required to sign the IACR copyright and consent form (available at `https://www.iacr.org/docs/`) 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 8, 2017, 22:00 EST**
- Paper notification: May 8, 2017
- Final version due: June 5, 2017
- Conference dates: August 20–24, 2017

Awards

The Program Committee may choose one or more papers to receive a “Best Paper” award, and may also choose to award a prize for the best paper authored exclusively by young researchers (i.e., researchers who have not received a PhD by August 2014). 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. 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. Requests for waivers and/or stipends should be addressed to the General Chair and not to the Program Chairs.

Program Committee

M. Abe, NTT Secure Platform Laboratories
S. Agrawal, IIT Madras
A. Akavia, The Academic College of Tel Aviv-Yaffo
E. Andreeva, KU Leuven
M. Bellare, UC San Diego
D. Boneh, Stanford University
E. Boyle, IDC Herzliya
R. Canetti, Boston University/Tel Aviv University
J.H. Cheon, Seoul National University
D. Dachman-Soled, University of Maryland
I. Damgård, Aarhus University
N. Döttling, UC Berkeley
O. Dunkelman, University of Haifa
E. Fujisaki, NTT Secure Platform Laboratories
S. Gorbunov, University of Waterloo
V. Goyal, Carnegie Mellon University
M. Green, Johns Hopkins University
N. Heninger, University of Pennsylvania
V.T. Hoang, Florida State University
D. Hofheinz, Karlsruhe Institute of Technology
S. Ionica, Université de Picardie
T. Iwata, Nagoya University
S. Kamara, Brown University
G. Leurent, Inria
H. Lin, UC Santa Barbara
S. Lucks, Bauhaus-Universität Weimar
V. Lyubashevsky, IBM Zurich
M. Mahmoody, University of Virginia
P. Mohassel, Visa Research
C. Orlandi, Aarhus University
E. Oswald, University of Bristol
R. Pass, Cornell University
G. Rose, TargetProof LLC
C. Schaffner, U. Amsterdam/CWI/QuSoft
G. Segev, Hebrew University
Y. Seurin, ANSSI
D. Stebila, McMaster University
S. Tessaro, UC Santa Barbara
M. Tibouchi, NTT Secure Platform Laboratories
E. Tromer, Tel Aviv University/Columbia University
D. Unruh, University of Tartu
V. Zikas, Rensselaer Polytechnic Institute

Advisory Member: Matt Robshaw, Impinj, Inc., Crypto 2016 Program Co-Chair

Contact Information

General Chair:
Steven Myers
Dept. of Computer Science and Informatics
Indiana University
Bloomington, IN 47408, USA
`crypto2017@iacr.org`

Program Co-Chairs:

Jonathan Katz
Dept. of Computer Science
University of Maryland
College Park, MD 20742, USA

Hovav Shacham
Dept. of Computer Science and Engineering
UC San Diego
La Jolla, CA 92093, USA

`crypto2017programchairs@iacr.org`