Crypto 2016 Call for Papers

Original contributions on all technical aspects of cryptology are solicited for submission to Crypto 2016, the 36th Annual International Cryptology Conference. Submissions are welcome on any cryptographic topic including, but not limited to:

- foundational theory,
- the design, proposal, and analysis of cryptographic primitives,
- secure implementation and optimization,
- industry applications and innovative "out-of-the-box" proposals.

Crypto 2016 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 2016 will be published by Springer in the LNCS series.

Instructions for Authors

Submissions must be at most 30 pages using the Springer LNCS format, including title page, references, 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.

Submissions should begin with a title, a short abstract, and a list of keywords. The introduction should summarize the contribution of the paper so that it is understandable to a non-expert in the field. 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 anonymous, with no author names, affiliations, or obvious references. All submissions will be blind-refereed and submissions must not substantially duplicate published work or work that has been submitted in parallel to any other journal or conference/workshop with proceedings. All submissions to Crypto 2016 are viewed as active submissions throughout the entire review period; they cannot be submitted to any other journal or conference/workshop with proceedings before the notification date. Accepted submissions cannot appear in any other conference or workshop that has proceedings. The IACR reserves the right to share information about submissions with other Program Committees. The IACR *Policy on Irregular Submissions* as well as *Guidelines for Authors* and other resources are all available via `www.iacr.org/docs/`.

Papers must be submitted electronically; a detailed description of the electronic submission procedure is available via the conference web-page. Submissions not meeting any of the guidelines above risk rejection without consideration of their merits. All accepted papers must conform to Springer publishing requirements and authors will be required to sign the IACR Copyright form when submitting the proceedings version of their papers. Authors must guarantee that their paper, if accepted, will be presented by one of the authors.

- Submission deadline: **February 9, 2016, 23:00 UTC (3:00 pm PST)**
- Paper notification: May 6, 2016
- Final version due: June 3, 2016
- Conference dates: August 14 – 18, 2016

Paper 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 for a PhD or have received their PhD degree in 2014 or later. As usual, awards will only be given if deserving papers are identified.

Stipends

The 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 those students unable to obtain funding to attend the conference. Students in under-represented groups are especially encouraged to apply. Requests for stipends should be addressed to the General Chair and not to the Program Chairs.

Program Committee

A. Biryukov, University of Luxembourg, LU.

A. Canteaut, INRIA, FR.

D. Catalano, Università di Catania, IT.

N. Chandran, Microsoft Research, IN.

M. Chase, Microsoft Research, US.

J. Daemen, STMicroelectronics, BE and Radboud University, NL.

E. De Mulder, Cryptographic Research, FR.

M. van Dijk, University of Connecticut, US.

I. Dinur, Ben-Gurion University, IL.

P.-A. Fouque, Université de Rennes 1, FR.

S. Galbraith, Auckland University, NZ.

S. Garg, University of California, Berkeley, US.

D. Gordon, George Mason University, US.

J. Groth, University College London, UK.

S. Ionica, Université de Picardie, FR.

T. Iwata, Nagoya University, JP.

A. Kiayias, National and Kapodistrian University of Athens, GR.

G. Leander, Ruhr Universität Bochum, DE.

S. Liu, Shanghai Jiao Tong University, CN.

A. May, Ruhr Universität Bochum, DE.

W. Meier, University of Applied Science, CH.

P. Mohassel, Yahoo Labs, US.

S. Myers, Indiana University, US.

P. Nguyen, Inria, FR and CNRS/JFLI and University of Tokyo, JP.

K. Nyberg, Aalto University, FI.

K. Paterson, Royal Holloway Univ. of London, UK.

T. Peyrin, Nanyang Technological University, SG.

B. Pinkas, Bar Ilan University, IL.

D. Pointcheval, Ecole Normale Superieure, FR.

M. Prabhakaran, University of Illinois, US.

B. Preneel, KU Leuven, BE.

M. Raykova, Yale University, US.

C. Rechberger, TU-Graz, AT and DTU, DK.

M. Rosulek, Oregon State University, US.

R. Safavi-Naini, University of Calgary, CA.

A. Scafuro, Boston University, US and Northeastern University, US.

P. Schaumont, Virginia Tech, US.

D. Schröder, CISPA, Saarland University, DE.

J. H. Seo, Myongji University, KR.

Y. Seurin, ANSSI, FR.

A. Shelat, University of Virginia, US.

N. Smart, University of Bristol, UK.

R. Steinfeld, Monash University, AU.

M. Tibouchi, NTT Secure Platform Laboratories, JP.

Advisory Member: Rosario Gennaro, The City College of New York, Crypto 2015 Program Co-Chair

Contact Information

General Chair:

Brian LaMacchia
Microsoft Research
One Microsoft Way
Redmond, WA 98052, US
crypto2016@iacr.org

Program Co-chairs:

Matt Robshaw
Impinj, Inc
400 Fairview Ave N
Suite 1200
Seattle, WA 98109, US

Jonathan Katz
University of Maryland
Department of Computer Science
8223 Paint Branch Dr.
College Park, MD 20742, US

crypto2016programchairs@iacr.org