Crypto 2015 Call for Papers

Original contributions on all technical aspects of cryptology are solicited for submission to Crypto 2015, the 35th 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,
- implementation security and optimization,
- industry application, and innovative "out-of-the-box" proposals.

Crypto 2015 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 2015 will be published by Springer in the LNCS series.

Instructions for Authors

Submissions must be at most 18 pages using the Springer LNCS format, excluding references and any supplementary material. Details on the LNCS format can be obtained via `www.springer.com/lncs`. The final published version of an accepted paper is expected to closely match these 18 pages.

Submissions must be submitted electronically and the submission procedure is described on the conference webpage. All submissions will be blind-refereed and submissions must be anonymous, with no author names, affiliations, or obvious references. They 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. Optionally, if an author desires, a clearly-marked appendix containing supplementary material can be appended to the submission after the references. This appendix has no prescribed form or page limit and might be used, for instance, to provide program code or additional experimental data. However reviewers are not required to read or review any supplementary material and submissions are expected to be intelligible and complete without it.

The IACR *Policy on Irregular Submissions* is available via `www.iacr.org/docs/`. Submissions must not substantially duplicate published work or work that has been submitted in parallel before, or during Crypto 2015 review, to any other journal or conference/workshop with proceedings. Accepted submissions cannot appear in any other conference or workshop that has proceedings. The program chairs may share information about submitted papers with other conference chairs to ensure adherence to this policy.

Accepted papers must conform to Springer publishing requirements and authors will be required to sign the IACR Copyright form. Authors must guarantee that their paper, if accepted, will be presented at the conference by one of the authors.

Important Dates

- Submission deadline: **February 11, 2015, 22:00 UTC (5:00 pm EST)**
- Paper notification: May 9, 2015
- Final version due: June 12, 2015
- Conference dates: August 16 – 20, 2015

Best Paper Awards

The Program Committee may award an overall best paper award. In a continuing effort to promote independent work by young researchers, the Program Committee may also award a prize for the best paper that is authored exclusively by young researchers. To be eligible, all co-authors must be either full-time students or have received their PhD degree in 2013 or later. As usual, awards will be given only if deserving papers are identified.

Stipends

The Cryptography Research Fund allows us to waive the registration fee for all students presenters of an accepted paper. A limited number of stipends will be available to those students unable to obtain funding to attend the conference, and to students having an accepted paper that they will present. Students in under-represented groups are especially encouraged to apply. Requests for stipends should be addressed to the General Chair.

Program Committee

M. Abdalla, École Normale Supérieure & CNRS, FR.
M. Abe, NTT Labs, JP.
P. Barreto, University of Sao Paulo, BR.
C. Boyd, Norwegian University of Science and Technology, NO.
Z. Brakerski, Weizmann Institute of Science, IL.
E. Bresson, Airbus Cybersecurity, FR.
A. Canteaut, INRIA, FR.
D. Catalano, Università di Catania, IT.
N. Chandran, Microsoft Research, IN.
M. Chase, Microsoft Research, US.
J. Daemen, STMicroelectronics, BE.
K. El Defrawy, HRL Laboratories, US.
O. Dunkelman, University of Haifa, IL.
D. Fiore, IMDEA Software Institute, ES.
S. Galbraith, Auckland University, NZ.
S. Garg, University of California, Berkeley, US.
C. Hazay, Bar-Ilan University, IL.
T. Iwata, Nagoya University, JP.
S. Jarecki, University of California, Irvine, US.
T. Johansson, Lund University, SE.
L.R. Knudsen, Technical University of Denmark, DK.
G. Leander, Ruhr-Universität Bochum, DE.
A. Bishop Lewko, Columbia University, US.
H. Lin, University of California, Santa Barbara, US.
M. Matsui, Mitsubishi Electric, JP.
S. Meiklejohn, University College London, UK.
D. Micciancio, University of California, San Diego, US.
S. Myers, Indiana University, US.
B. Parno, Microsoft Research, US.
G. Persiano, Università di Salerno, IT.
T. Peyrin, Nanyang Technological University, SG.
J. Pieprzyk, Queensland University of Technology, AU.
A. Poschmann, NXP Semiconductors, DE.
B. Preneel, KU Leuven, BE.
C. Ràfols, Ruhr-Universität Bochum, DE.
M. Raykova, SRI International, US.
P. Sarkar, Indian Statistical Institute, IN.
N. Smart, University of Bristol, UK.
F.-X. Standaert, Université catholique de Louvain, BE.
J. Steinberger, Tsinghua University, CN.

Advisory Member: Juan Garay, Yahoo Labs, Crypto 2014 Program Co-Chair

Contact Information

General Chair: **Thomas Ristenpart**
University of Wisconsin, Madison
1210 West Dayton Street,
Madison, WI 53715, US
crypto2015@iacr.org

Program Chairs: **Rosario Gennaro**
The City College of New York
Shepard Hall, 279
160 Convent Avenue, New York
NY 10031, US

Matt Robshaw
Impinj, Inc
701 N. 34th Street, Suite 300
Seattle
WA 98103, US

crypto2015programchairs@iacr.org