www.mta.ca/sac2015

SAC 2015 — Call for Papers

Authors are encouraged to submit original papers related to the following themes for the SAC 2015 conference. Note that the first three are traditional SAC areas, and the fourth topic is the special focus for this year.

- Design and analysis of symmetric key primitives and cryptosystems, including block and stream ciphers, hash functions, MAC algorithms, and authenticated encryption schemes.
- Efficient implementations of symmetric and public key algorithms.
- Mathematical and algorithmic aspects of applied cryptology.
- *Privacy and anonymity enhancing technologies and their analysis.*

In Cooperation with IACR

Instructions for Authors

- Papers must be submitted electronically. Submission details will be given on the conference web site.
- Submissions must be anonymous, with no author names, affiliations, acknowledgments, or obvious references.
- Papers should be at most 12 pages in length, excluding bibliography and appendices, and use single-column format, reasonable margins, and at least 11-point fonts. Total length must not exceed 24 pages. Committee members are not required to read appendices, so the paper should be intelligible without them.
- Papers must be written in English, and begin with a title, a short abstract, and a list of keywords.
- The introduction should summarize the paper's contributions at a level appropriate for a non-specialist reader.
- Submissions should be in PDF format. As the conference proceedings will be published by Springer, we recommend that submissions be typeset using LaTeX and the LNCS style available on the Springer LNCS web site.
- If at all possible, the paper should use Type 1 (outline) fonts rather than Type 3 (bitmap) fonts.

Submissions must not substantially duplicate work that any of the authors has published elsewhere or has submitted in parallel to a journal or any other conference/workshop that has proceedings. The SAC Chairs reserve the right to share information about submissions with other program committees or journal editors to detect parallel submissions. In addition, the SAC Chairs reserve the right to contact an author's institution/corporation and/or other appropriate organizations if an irregular submission is detected.

Papers not meeting these guidelines risk rejection without consideration of their merits. Neither late submissions, submissions by email, nor hardcopy submissions will be accepted. Submission implies the commitment of at least one of the authors to present the paper. The SAC Chairs reserve the right to withdraw papers from the proceedings that are not presented at the conference.

Important Dates

- Paper submission deadline: **May 25, 2015, 19:00 GMT**
- Notification of decision: July 6, 2015
- Pre-proceedings version deadline: July 27, 2015
- Conference dates: August 12–14, 2015

SAC 2015 Program Committee

- Carlisle Adams, University of Ottawa, Canada
- Elena Andreeva, KU Leuven, Belgium
- Jean-Philippe Aumasson, Kudelski Security, Switzerland
- Roberto Avanzi, Qualcomm, Germany
- Paulo S.L.M. Barreto, University of Sao Paulo, Brazil
- Josh Benaloh, Microsoft Research, USA
- Daniel J. Bernstein, University of Illinois at Chicago, USA, and TU Eindhoven, Netherlands
- John Black, University of Colorado at Boulder, USA
- Nikita Borisov, University of Illinois at Urbana-Champaign, USA
- Itai Dinur, École Normale Supérieure, France
- Orr Dunkelman, University of Haifa, Israel **(Co-Chair)**
- Guang Gong, University of Waterloo, Canada
- Tim Güneysu, Ruhr-University Bochum, Germany
- Seda Gürses, New York University, USA
- Michael Jacobson, University of Calgary, Canada
- Antoine Joux, Paris 6, France
- Nathan Keller, Bar Ilan University, Israel
- Liam Keliher, Mount Allison University, Canada **(Co-Chair)**
- Tanja Lange, TU Eindhoven, Netherlands
- Gregor Leander, Ruhr-University Bochum, Germany
- Anja Lehmann, IBM Research Zurich, Switzerland
- Petr Lisonek, Simon Fraser University, Canada
- Florian Mendel, TU Graz, Austria
- María Naya-Plasencia, INRIA, France
- Kaisa Nyberg, Aalto University, Finland
- Christian Rechberger, TU Denmark, Denmark
- Dipanwita Roy Chowdhury, IIT Kharagpur, India
- Palash Sarkar, Indian Statistical Institute, India
- Meltem Sönmez Turan, NIST, USA
- Douglas Stinson, University of Waterloo, Canada
- Carmela Troncoso, Gradiant, Spain
- Vanessa Vitse, Institut Fourier, Université de Grenoble I, France
- Bo-Yin Yang, Academia Sinica, Taiwan
- Amr Youssef, Concordia University, Canada
- Moti Yung, Google, USA

Stipends and Visas

Authors who are unable to attend for financial reasons, in particular student authors, should note the possibility of requesting a stipend. Authors requiring a visa may ask for an invitation letter before notification of acceptance.

Contact

Please direct all inquiries to: **sac2015 at mta.ca**

SAC Summer School (S3), August 10–12, 2015

In 2015, for the first time, SAC will be preceded by the **SAC Summer School (S3)**. The purpose of S3 is to provide participants with an opportunity to gain in-depth knowledge of specific areas of cryptography related to the current SAC topics by bringing together world-class researchers who will give extended talks in their areas of specialty. S3 is designed to create a focused learning environment that is also relaxed and collaborative. The SAC Summer School is open to all attendees, and may be of particular interest to students, postdocs, and other early researchers

For more information, visit: **mta.ca/sac2015/s3.html**

SAC and S3 SPONSORS: