SAC 2018 – Call for Papers

www.ucalgary.ca/cpsc/sac2018

The 25th Conference on Selected Areas in Cryptography (SAC 2018) will take place at the University of Calgary in Alberta, Canada on August 15-17, 2018. SAC 2018 is held in cooperation with the International Association for Cryptologic Research (IACR).

Authors are encouraged to submit original papers related to the following themes for SAC 2018. Note that the first three are traditional SAC areas; 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.
- *Cryptography for the Internet of Things.*

Instructions for Authors

- Papers must be submitted electronically, via the submission webpage at https://easychair.org/conferences/?conf=sac2018. Late submissions, submissions by email, or hardcopy submissions will not be accepted.
- Submissions must be anonymous, with no author names, affiliations, acknowledgments or obvious references.
- Papers should be at most 16 pages in length, excluding bibliography and clearly marked appendices and typeset using LaTeX and the LNCS style (available on the Springer LNCS website). Total length must not exceed 24 pages. Program 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. An introduction section should summarize the paper's contributions at a level appropriate for a non-specialist reader.
- Submissions should be in PDF format. 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 2018 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. Submissions not meeting these guidelines risk rejection without consideration of their merits. For further details, please refer to the IACR Policy on Irregular Submissions at https://www.iacr.org/docs/irregular.pdf.

Authors, program committee members, and reviewers for SAC 2018 must adhere to the IACR Policy on Conflicts of Interest. Authors are requested to identify all members of the SAC 2018 Program Committee who have an automatic conflict of interest (COI) with the submission, and disclose it to the chairs by email to sac2018.pc.chair@gmail.com at the time of submission. It is the responsibility of all authors to ensure correct reporting of COI information. Submissions with incorrect or incomplete COI information may be rejected without consideration of their merits. For further details, please refer to the IACR Policy on Conflicts of Interest at https://www.iacr.org/docs/conflicts.pdf.

Submission implies the commitment of at least one of the authors to present the paper at the conference. The SAC 2018 Chairs reserve the right to withdraw papers from the proceedings that are not presented at the conference. The SAC 2018 proceedings will be published by Springer in the Lecture Notes in Computer Science series.

Important Dates

- **Submission deadline:** **9 May 2018 (23:59 UTC)**
- Notifications: 27 June 2018
- Pre-proceedings version deadline: 18 July 2018
- SAC Summer School: 13-14 August 2018
- Conference: 15-17 August 2018

SAC 2018 Program Committee

- Carlisle Adams, University of Ottawa, Canada
- Diego Aranha, University of Campinas, Brazil
- Frederik Armknecht, Universität Mannheim, Germany
- Roberto Avanzi, ARM, Germany
- Steve Babbage, Vodafone, UK
- Paulo Barreto, University of Washington Tacoma, USA
- Daniel J. Bernstein, University of Illinois at Chicago, USA
- Alex Biryukov, University of Luxembourg, Luxembourg
- Andrey Bogdanov, DTU, Denmark
- Carlos Cid, Royal Holloway, University of London, UK (**CHAIR**)
- Vassil Dimitrov, University of Calgary, Canada
- Itai Dinur, Ben-Gurion University, Israel
- Maria Eichlseder, TU Graz, Austria
- Pierre-Alain Fouque, Univ Rennes and Institut Universitaire de France, France
- Guang Gong, University of Waterloo, Canada
- Johann Groszschaedl, University of Luxembourg, Luxembourg
- M. Anwar Hasan, University of Waterloo, Canada
- Howard Heys, Memorial University of Newfoundland, Canada
- Jérémy Jean, ANSSI, France
- Elif Bilge Kavun, Infineon Technologies, Germany
- Stefan Kölbl, DTU, Denmark
- Gaëtan Leurent, INRIA, France
- Subhamoy Maitra, Indian Statistical Institute, India
- Brice Minaud, Royal Holloway, University of London, UK
- Nicky Mouha, NIST, USA
- Michael Naehrig, Microsoft Research, USA
- Svetla Nikova, KU Leuven, Belgium
- Ludovic Perret, Sorbonne University/INRIA/CNRS, France
- Josef Pieprzyk, Data61, CSIRO, Australia
- Francesco Regazzoni, Università della Svizzera Italiana, Switzerland
- Matt Robshaw, Impinj, USA
- Sondre Rønjom, University of Bergen, Norway
- Fabrizio De Santis, Siemens AG, Germany
- Sujoy Sinha Roy, KU Leuven, Belgium
- Jörn-Marc Schmidt, secunet Security Networks, Germany
- Peter Schwabe, Radboud University, Netherlands
- Kyoji Shibutani, Sony Corporation, Japan
- Paul Stankovski, Lund University, Sweden
- Frederik Vercauteren, KU Leuven, Belgium
- Meiqin Wang, Shandong University, China
- Hongjun Wu, Nanyang Technological University, Singapore
- Huapeng Wu, University of Windsor, Canada
- Bo-Yin Yang, Academia Sinica, Taiwan
- Kan Yasuda, NTT, Japan
- Amr Youssef, Concordia University, Canada

Stipends and Visas

Authors of accepted papers – particularly student authors – who are unable to attend the conference for financial reasons, may contact the organizers to apply for financial support*.
Conference attendees should refer to the conference website at www.ucalgary.ca/cpsc/sac2018 to obtain information about visa requirements to attend SAC 2018.

SAC Summer School (S3)

S3 will be held prior to SAC 2018, on August 13-14, at the University of Calgary.

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 (half-day or full-day) in their areas of expertise. 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-career researchers.

For more information about this year's S3, visit www.ucalgary.ca/cpsc/selected-areas-cryptography/summer-school.

SAC 2018 Organizing Committee

Mike Jacobson - Local Co-Chair
Department of Computer Science
University of Calgary
Calgary, Alberta, Canada

Carlos Cid - External (Program) Co-Chair
Information Security Group
Royal Holloway, University of London
Egham, Surrey, UK

General enquiries about SAC 2018, including requests for invitation letters and questions about registration, should be sent to sac2018@ucalgary.ca.

* award of stipends is subject to availability of funds.