SAC **SELECTED AREAS IN CRYPTOGRAPHY 2019**

UNIVERSITY OF WATERLOO

Call for Papers

The 26th Conference on Selected Areas in Cryptography (SAC 2019) will take place at the University of Waterloo in Waterloo, Ontario, Canada on August 14-16, 2019, and will be preceded by the SAC Summer School on August 12-13, 2019. SAC 2019 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 2019. Note that the first three are traditional SAC areas; the fourth topic is the special focus for this year.

1. Design and analysis of symmetric key primitives and cryptosystems, including block and stream ciphers, hash functions, MAC algorithms, and authenticated encryption schemes.
2. Efficient implementations of symmetric and public key algorithms.
3. Mathematical and algorithmic aspects of applied cryptology.
4. Real-world cryptography / cryptographic protocols in practice.

SAC 2019 also welcomes papers in any of the areas above with a focus on post-quantum cryptography.

The SAC 2019 proceedings will be published by Springer in the Lecture Notes in Computer Science series.

Instructions for Authors

- Papers must be submitted electronically; a submission link will be made available at https://uwaterloo.ca/sac-2019/ no later than April 1, 2019. 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 must be typeset using LaTeX in the LNCS style (https://www.springer.com/gp/computer-science/lncs/conference-proceedings-guidelines) with no alterations to font size or margins, with the exception of using `\pagestyle{plain}` to add page numbers. The main body of the paper must be at most 20 pages in length; including bibliography and clearly marked appendices, the total length must not exceed 30 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 must be in PDF format.

Submission implies the commitment of at least one of the authors to present the paper at the conference. The SAC 2019 Chairs reserve the right to withdraw papers from the proceedings that are not presented at the conference or for which the camera-ready post-proceedings version is not submitted by the deadline.

Irregular submissions. SAC 2019 follows the IACR's Policy on Irregular Submissions. 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 2019 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.

Conflicts of interest. SAC 2019 follows the IACR's Policy on Conflicts of Interest (COI). Authors, program committee members, and reviewers for SAC 2019 must adhere to the IACR Policy on Conflicts of Interest. Authors are requested to identify all members of the SAC 2019 Program Committee who have an automatic conflict of interest with the submission, and disclose it 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.

Code of conduct. SAC 2019 is committed to providing an experience free of harassment and discrimination, respecting the dignity of every participant. Participants who violate this code may be sanctioned and/or expelled from the event, at the discretion of the Chairs. Serious incidents may be referred to the IACR Ethics Committee for further possible action. Any action will only be taken with the consent of the affected party subject to applicable laws.

If you experience harassment or discriminatory behaviour at SAC 2019, we encourage you to reach out to either of the SAC 2019 Chairs or the Chair of the SAC Board (Michael Jacobson <jacobs@ucalgary.ca>).

If you witness harassment or discriminatory behaviour, please consider intervening.

Important Dates

- **Submission deadline**: Fri May 3 2019, 23:59:59 UTC-1200 – **No extensions!** (Convert to local time)
- Notification: Mon Jun 17 2019
- Pre-proceedings version deadline: Mon Jul 15 2019
- SAC Summer School: Mon Aug 12 - Tue Aug 13 2019
- Conference: Wed Aug 14 - Fri Aug 16 2019
- Camera-ready post-proceedings version deadline: Tue Sep 17 2019

Program Committee

- Andreas Hülsing, Eindhoven University of Technology, The Netherlands
- Atefeh Mashatan, Ryerson University, Canada
- Atul Luykx, Visa Research, USA
- Bart Mennink, Radboud University, The Netherlands
- Benjamin Dowling, Royal Holloway, University of London, UK
- Bertram Poettering, Royal Holloway, University of London, UK
- Chris Peikert, University of Michigan, USA
- Christophe Petit, University of Birmingham, UK
- Craig Costello, Microsoft Research, USA
- Diego Aranha, Aarhus University, Denmark / University of Campinas, Brazil
- Douglas Stebila, University of Waterloo, Canada (co-chair)
- Fabrice Benhamouda, IBM Research, USA
- Fang Song, Texas A&M University, USA
- Gareth T. Davies, University of Paderborn, Germany
- Giorgia Azzurra Marson, NEC Laboratories Europe, Germany
- Guang Gong, University of Waterloo, Canada
- Javad Doliskani, University of Waterloo, Canada
- Jean Paul Degabriele, TU Darmstadt, Germany
- Joppe W. Bos, NXP Semiconductors, Belgium
- Juraj Somorovsky, Ruhr-Universität Bochum, Germany
- Kan Yasuda, NTT, Japan
- Kenneth G. Paterson, Royal Holloway, University of London, UK / ETH Zürich, Switzerland (co-chair)
- Leonie Simpson, Queensland University of Technology, Australia
- Máire O'Neill, CSIT, Queen's University Belfast, UK
- Marc Joye, OneSpan, Belgium
- Marcel Keller, Data61, Australia
- Mridul Nandi, Indian Statistical Institute, Kolkata, India
- Nele Mentens, KU Leuven, Belgium

- Orr Dunkelman, University of Haifa, Israel
- Patrick Longa, Microsoft Research, USA
- Paul Grubbs, Cornell Tech, USA
- Paulo Barreto, University of Washington Tacoma, USA
- Reihaneh Safavi-Naini, University of Calgary, Canada
- Renate Scheidler, University of Calgary, Canada
- Somitra Kumar Sanadhya, Indian Institute of Technology Ropar, India
- Takanori Isobe, University of Hyogo & NICT, Japan
- Tarik Moataz, Brown University, USA
- Tibor Jager, Universität Paderborn, Germany
- Tim Güneysu, Ruhr-Universität Bochum & DFKI, Germany
- Tomer Ashur, KU Leuven, Belgium
- Vadim Lyubashevsky, IBM Research, Switzerland
- Willi Meier, FHNW, Switzerland
- Yosuke Todo, NTT Secure Platform Laboratories, Japan
- Yuval Yarom, University of Adelaide and Data61, Australia
- Zhenfeng Zhang, Institute of Software, Chinese Academy of Sciences, China

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. Stipends subject to availability of funds.

Conference attendees should refer to the conference website and the Government of Canada website (https://www.canada.ca/en/immigration-refugees-citizenship/services/visit-canada.html) for information about visa requirements to attend SAC 2019. Submitters who may require visas are encouraged to begin the process early, and in particular can contact the organizers after submission but prior to the notification deadline to request a letter of invitation.

SAC Summer School

The SAC Summer School will be held prior to SAC, on August 12-13, 2019, at the University of Waterloo. The purpose of the SAC Summer School 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) in their areas of specialty. 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 SAC Summer School, visit https://uwaterloo.ca/sac-2019/.

SAC 2019 Organizing Committee

Douglas Stebila – Co-Chair
Department of Combinatorics & Optimization
University of Waterloo
Waterloo, Ontario, Canada

Kenneth G. Paterson – Co-Chair
Information Security Group
Royal Holloway, University of London
Egham, Surrey, UK
and
ETH Zürich
Zürich, Switzerland

General enquiries about SAC 2019, including requests for invitation letters and questions about registration, should be sent to sac2019chairs@gmail.com.