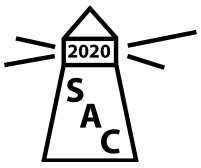
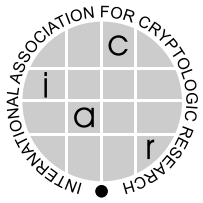
Selected Areas in Cryptography (SAC) 2020

Call for Papers



The 27th Conference on Selected Areas in Cryptography (SAC 2020) will take place as an online conference on October 21–23, 2020, and will be preceded by the SAC "Summer" School on October 19–20, 2020. SAC 2020 is held in cooperation with the International Association for Cryptologic Research (IACR).



Authors are encouraged to submit original papers related to the following three regular topics for SAC 2020:

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.

In addition, the following topic as the special topic for SAC 2020:

4. Secure Elections and Related Cryptographic Constructions

SAC 2020 also welcomes papers in any of the areas above with a focus on post-quantum cryptography.

The SAC 2020 proceedings will be published by Springer in the Lecture Notes in Computer Science series.

Instructions for Authors

- Papers must be submitted electronically; the submission link will be made available at https://sac2020.ca/. 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. It is possible to have clearly marked appendices, as long as the total length of the paper does 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. Note that due to the COVID-19 pandemic, the conference will be held in an online manner. The SAC 2020 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 2020 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 2020 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 2020 follows the IACR's Policy on Conflicts of Interest (COI). Authors, program committee members, and reviewers for SAC 2020 must adhere to the IACR Policy on Conflicts of Interest. Authors are requested to identify all members of the SAC 2020 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. While being held as an online event, SAC 2020 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 as well as to the relevant enforcement agency. Any action will only be taken with the consent of the affected party subject to applicable laws.

If you experience harassment or discriminatory behavior at SAC 2020, we encourage you to reach out to any of the SAC 2020 Chairs.

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

Important Dates

- **Submission deadline**: Tuesday, August 11 2020, 23:59:59 UTC-1200 – **No extensions!** (Convert to local time)
- Notification: Thursday September 17 2020
- Pre-proceedings version deadline: Thursday October 8 2020
- SAC Summer School: Monday 19 – Tuesday 20 October 2020
- Conference: Wed October 21 – Friday October 23 2020
- Camera-ready post-proceedings version deadline: Tuesday December 1 2020

Program Committee

- Riham AlTawy, University of Victoria, Canada
- Diego Aranha, Aarhus University, Denmark
- Tomer Ashur, TU Eindhoven, the Netherlands and KU Leuven, Belgium
- Roberto Avanzi, ARM, Germany
- Paulo Barreto, University of Washington Tacoma, USA
- Josh Benaloh, Microsoft Research, USA
- Daniel J. Bernstein, University of Illinois at Chicago, USA and Ruhr University Bochum, Germany
- Jean-François Biasse, University of South Florida, USA
- Claude Carlet, Université Paris 8, France and University of Bergen, Norway
- Carlos Cid, Royal Holloway, University of London, UK and Simula UiB, Norway
- Orr Dunkelman (co-chair), University of Haifa, Israel
- Aleksander Essex, Western University, Canada
- Maria Eichlseder, Graz University of Technology, Austria
- Ryan Henry, University of Calgary, Canada
- Howard Heys, Memorial University, Canada
- Michael J. Jacobson Jr. (co-chair), University of Calgary, Canada
- Marcel Keller, Data61, Australia
- Yunwen Liu, National University of Defense Technology, China
- Subhamoy Maitra, Indian Statistical Institute Kolkata, India
- Kalikinkar Mandal, University of New Brunswick, Canada
- Atefeh Mashatan, Ryerson University, Canada
- Barbara Masucci, University of Salerno, Italy
- Abderrahmane Nitaj, University of Caen Normandy, France
- Colin O'Flynn (co-chair), Dalhouise University, Canada
- Christiane Peters, IBM, Belgium
- Christophe Petit, University of Birmingham, UK
- Olivier Pereira, Université Catholique de Louvain, Belgium
- Elizabeth Quaglia, Royal Holloway, University of London, UK
- Francisco Rodríguez-Henríquez, CINVESTAV, Mexico

- Eyal Ronen, Tel Aviv University, Israel
- Tobias Schneider, NXP Semiconductors, Austria
- Nicolas Sendrier, Inria, France
- Leonie Simpson, Queensland University of Technology, Australia
- Benjamin Smith, Inria and École polytechnique, Institut Polytechnique de Paris, France
- Djiby Sow, Cheikh Anta Diop University, Senegal
- Martijn Stam, Simula UiB, Norway
- Douglas Stebila, University of Waterloo, Canada
- Vanessa Teague, Australian National University and Thinking Cybersecurity, Australia
- Yosuke Todo, NTT Secure Platform Laboratories, Japan
- Yuntao Wang, Japan Advanced Institute of Science and Technology, Japan
- Huapeng Wu, University of Windsor, Canada

SAC "Summer" School

The SAC Summer School will be held prior to SAC, on October 19–20, 2020, in an online manner. 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://sac2020.ca/summerschool.html.

SAC 2020 Organizing Committee

Colin O'Flynn – Co-Chair
Department of Electrical
and Computer Engineering
Dalhouise University
Halifax, Nova Scotia, Canada

Michael J. Jacobson Jr. – Co-Chair
Department of Computer Science,
University of Calgary,
Calgary, Alberta, Canada

Orr Dunkelman– Co-Chair
Department of Computer Science,
University of Haifa,
Haifa, Israel

General enquiries about SAC 2020, including questions about registration, should be sent to sac2020chairs@gmail.com.