Selected Areas in Cryptography (SAC) 2022

Call for Papers

The 29th Conference on Selected Areas in Cryptography (SAC 2022) will take place in Windsor, Ontario, Canada, on August 24 – August 26, 2022, and will be preceded by the SAC "Summer" School on August 22-23, 2022. Depending on the circumstances, the conference can run in hybrid mode (both in-person and virtual).

SAC 2022 is held in cooperation with the International Association for Cryptologic Research (IACR).

Topics & Proceedings

Authors are encouraged to submit original papers related to the following three regular topics for SAC 2022:

- 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, public key, and post-quantum cryptography.
- Mathematical and algorithmic aspects of applied cryptology, including post-quantum cryptology.

In addition, the following topic as the special topic for SAC 2022:

- Theory and practice of isogeny-based cryptography.

The SAC 2022 proceedings will be published by Springer in the Lecture Notes in Computer Science series.

Instructions for Authors

- Papers must be submitted electronically at https://easychair.org/conferences/?conf=sac2022. 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 with no alterations to font size or margins, with the exception of using 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. The SAC 2022 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 2022 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 2022 Chairs reserve the right to share information about submissions with other program committees or journal editors to detect parallel submissions. In addition, the SAC 2022 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.
- Conflicts of interest
  - SAC 2022 follows the IACR's Policy on Conflicts of Interest (COI). Authors, program committee members, and reviewers for SAC 2022 must adhere to the IACR Policy on Conflicts of Interest. Authors are requested to identify all members of the SAC 2022 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.
- Code of conduct
  - SAC 2022 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 2022, we encourage you to reach out to any of the SAC 2022 Chairs.
  - If you witness harassment or discriminatory behavior, please consider intervening.
- Submission Link
  - Please submit your paper at https://easychair.org/conferences/?conf=sac2022.

Important Dates

- Abstract registration deadline: June 1, 2022, 23:59 GMT
- Final paper submission deadline: June 8, 2022, 23:59 GMT
- Notification of decision: July 18, 2022
- Pre-proceedings version deadline: August 10, 2022
- 'Summer' School: August 22-23, 2022
- Conference dates: August 24-26, 2022

Program Committee

- Riham AlTawy, University of Victoria, Canada
- Melissa Azouaoui, NXP Semiconductors, USA
- Paulo Barreto, University of Washington Tacoma, USA
- Jean-François Biasse, University of South Florida, USA
- Olivier Blazy, École polytechnique, France
- Claude Carlet, Université Paris 8, France and University of Bergen, Norway
- Wouter Castryck, KU Leuven, Belgium
- Carlos Cid, Simula UiB, Norway and Okinawa Institute of Science and Technology, Japan
- Craig Costello, Microsoft Research, USA
- Luca De Feo, IBM Research Europe, Switzerland
- Maria Eichlseder, Graz University of Technology, Austria
- Aurore Guillevic, Inria Nancy, France and Aarhus University, Denmark
- Kathrin Hövelmanns, TU Eindhoven, the Netherlands
- Michael J. Jacobson Jr., University of Calgary, Canada
- Yunwen Liu, Independent
- Subhamoy Maitra, Indian Statistical Institute Kolkata, India
- Kalikinkar Mandal, University of New Brunswick, Canada
- Chloe Martindale, University of Bristol, UK
- Barbara Masucci, University of Salerno, Italy
- Ruben Niederhagen, Academia Sinica and University of Southern Denmark

- Abderrahmane Nitaj, University of Caen Normandy, France
- Lorenz Panny, Academia Sinica, Taipei, Taiwan
- Elizabeth A. Quaglia, Royal Holloway, University of London, UK
- Francisco Rodríguez-Henríquez, CINVESTAV-IPN, México and CRC-TII, United Arab Emirates
- Yann Rotella, Université de Versailles Saint-Quentin, France
- Simona Samardjiska, RU Nijmegen, the Netherlands
- Nicolas Sendrier, Inria, France
- Leonie Simpson, Queensland University of Technology, Australia
- Benjamin Smith (co-chair), Inria and École polytechnique, Institut Polytechnique de Paris, France
- Djiby Sow, Cheikh Anta Diop University, Senegal
- Douglas Stebila, University of Waterloo, Canada
- Katsuyuki Takashima, Waseda University, Japan
- Yosuke Todo, NTT Secure Platform Laboratories, Japan
- Yuntao Wang, Osaka University
- Huapeng Wu (co-chair), University of Windsor, Canada

Conference Co-chair

- Benjamin Smith, Inria and École polytechnique, Institut Polytechnique de Paris, France.
- Huapeng Wu, University of Windsor, Canada.

General Enquiries

General enquiries about SAC 2022, including questions about registration, should be sent to (email for SAC 2022)