Selected Areas in Cryptography 2013

http://sac2013.irmacs.sfu.ca/

14–16 August 2013 Burnaby, British Columbia, Canada

Call for Papers (updated deadline)

The **Conference on Selected Areas in Cryptography** (SAC) `http://sacconference.org/`, is an annual conference dedicated to specific themes in the area of cryptographic system design and analysis. It will take place in Burnaby, British Columbia, at Simon Fraser University on August 14–16, 2013. SAC 2013 is the 20th conference in this series, and for this special occasion will be extended to a 2.5 day conference, starting on the afternoon of August 14 with two invited talks. SAC 2013 is held in co-operation with the International Association for Cryptologic Research (IACR), which is the leading professional organization for cryptographic research.

Authors are encouraged to submit original papers related to the following themes for the SAC 2013 conference. Note that the first three are traditional SAC areas and the fourth topic varies from year to year.

- Design and analysis of symmetric key primitives and cryptosystems, including block and stream ciphers, hash functions, and MAC algorithms.
- Efficient implementations of symmetric and public key algorithms.
- Mathematical and algorithmic aspects of applied cryptology.
- Elliptic and hyperelliptic curve cryptography, including theory and applications of pairings.

Submissions must not substantially duplicate work that any of the authors has published elsewhere or has submitted in parallel to any other journal, conference, or workshop that has proceedings. Information about submissions may be shared with program chairs of other conferences for that purpose. Accepted submissions may not appear in any other conference or workshop that has proceedings.

The proceedings will be published in Springer-Verlag's Lecture Notes in Computer Science (LNCS) Series. The conference record will be available to participants during the conference in electronic form. Instructions about the preparation of a final proceedings version will be sent to the authors of accepted papers.

Paper submission deadline:	May 15 2013, 23:59 UTC
Modifications allowed until:	May 17 2013, 23:59 UTC
Notification of decision:	June 24, 2013
Preproceedings version deadline:	July 24, 2013
Conference:	August 14–16, 2013

Instructions for Authors

- Papers must be submitted electronically. Details on the submission process are given on the conference web site.
- The submission must be anonymous, with no author names, affiliations, acknowledgments, or obvious references.

- The authors are advised to not make substantial changes to the scope of their submission after May 15, reviewers will be chosen based on the submissions received by May 15.
- The length of the submission should be at most 12 pages excluding bibliography and appendices. It should be in single-column format, use at least 11-point fonts, and have reasonable margins. There is no page limit on the total length of the paper but accepted papers will be restricted to no more than 18 pages in LNCS style. Authors are encouraged to use this space to include proofs, source code, and other information allowing verification of results; unverifiable papers risk rejection. However, committee members will read beyond 12 pages at their discretion, so the submission should be intelligible without the appendices.
- The submission must be written in English, should begin with a title, a short abstract, and a list of keywords. The introduction should summarize the contributions of the paper at a level appropriate for a non-specialist reader. Committee members are not required to read appendices; the paper should be intelligible without them.
- As the conference proceedings will be published by Springer, we recommend that the submission be typeset using LaTeX and the LNCS style available from the Springer web site (follow the "For Authors" link). Submissions should be in PDF (a .pdf file) format.

Submissions not meeting these guidelines risk rejection without consideration of their merits. Neither late submissions, submissions by email, nor hardcopy submissions will be accepted. Authors of accepted papers must guarantee that their paper will be presented at the conference.

Program Committee

Carlisle Adams, University of Ottawa, Canada · Jean-Philippe Aumasson, Kudelski Security, Switzerland · Paulo S. L. M. Barreto, University of São Paulo, Brazil · Lejla Batina, Radboud University Nijmegen, Netherlands and KU Leuven, Belgium · Daniel J. Bernstein, University of Illinois at Chicago, USA and Technische Universiteit Eindhoven, Netherlands · Andrey Bogdanov, Technical University of Denmark, Denmark · Joppe Bos, Microsoft Research, USA · Christophe De Cannière, Google Switzerland, Switzerland · Anne Canteaut, INRIA Paris-Rocquencourt, France · Sanjit Chatterjee, Indian Institute of Science, India · Carlos Cid, Royal Holloway, University of London, UK · Craig Costello, Microsoft Research, USA · Joan Daemen, ST Microelectronics, Belgium · Vassil Dimitrov, University of Calgary, Canada · Orr Dunkelman, University of Haifa, Israel · Andreas Enge, INRIA Bordeaux-Sud-Ouest and University of Bordeaux, France · Matthieu Finiasz, CryptoExperts, France · Guang Gong, University of Waterloo, Canada · Tim Güneysu, Ruhr-University Bochum, Germany · Huseyin Hisil, Yasar University, Turkey · Sorina Ionica, ENS Paris, France · Mike Jacobson, University of Calgary, Canada · Dmitry Khovratovich, University of Luxembourg, Luxembourg · Tanja Lange, Technische Universiteit Eindhoven, Netherlands **(Co-chair)** · Kristin Lauter, Microsoft Research, USA **(Co-chair)** · Gregor Leander, Ruhr-University Bochum, Germany · Hyang-Sook Lee, Ewha Womans University, Republic of Korea · Jooyoung Lee, Faculty of Mathematics and Statistics, Sejong University, Seoul, Korea · Gaëtan Leurent, UCL Crypto Group, Belgium · Petr Lisoněk, Simon Fraser University, Canada **(Co-chair)** · Stefan Lucks, University Weimar, Germany · Alfred Menezes, University of Waterloo, Canada · Michael Naehrig, Microsoft Research, USA · María Naya-Plasencia, INRIA Paris-Rocquencourt, France · Kaisa Nyberg, Aalto University, Finland · Roger Oyono, Université de la Polynésie Française, French Polynesia · Daniel Page, University of Bristol, UK · Christiane Peters, Technical University of Denmark, Denmark · Bart Preneel, KU Leuven, Belgium · Christian Rechberger, Technical University of Denmark, Denmark · Christophe Ritzenthaler, Institut de Mathématiques de Luminy, France · Damien Robert, INRIA Bordeaux Sud-Ouest, France · Francisco Rodríguez-Henríquez, CINVESTAV-IPN, Mexico · Yu Sasaki, NTT Secure Platform Laboratories, Japan · Renate Scheidler, University of Calgary, Canada · Martin Schläffer, Graz University of Technology, Austria · Peter Schwabe, Radboud University Nijmegen, Netherlands · Douglas R. Stinson, University of Waterloo, Canada · Andrew Sutherland, MIT, USA · Vanessa Vitse, Université Joseph Fourier, France · Michael J. Wiener, Irdeto, Canada