SAC 2012 Call for Papers

August 16-17, 2012
Windsor, Ontario, Canada
http://uwindsor.ca/sac2012

The Conference on Selected Areas in Cryptography (SAC), previously called the Workshop on Selected Areas in Cryptography until 2011, is an annual conference dedicated to specific themes in the area of cryptographic system design and analysis. SAC 2012 will take place on August 16-17, 2012, at the University of Windsor, Windsor, Ontario, Canada.

Authors are encouraged to submit original papers related to the following themes for the SAC 2012 conference. Note that the first three are traditional SAC areas and the fourth topic is a new theme for this year's conference.

1. Design and analysis of symmetric key primitives and cryptosystems, including block and stream ciphers, hash functions, and MAC algorithms.
2. Efficient implementations of symmetric and public key algorithms.
3. Mathematical and algorithmic aspects of applied cryptology.
4. *Light-weight authentication protocols.*

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. As in previous years, the conference record will be available to participants during the conference. Instructions about the preparation of a final proceedings version will be sent to the authors of accepted papers.

Important Dates

Updated submission deadline:	**May 15, 2012 at 23:59 (11.59 pm) UTC/GMT**
Notification decision:	July 10, 2012
Preproceedings version deadline:	July 24, 2012
Conference:	August 16-17, 2012

Instructions for Authors

- Papers must be submitted electronically. Details about the submission process will be given on the conference web site.
- The submission must be anonymous, with no author names, affiliations, acknowledgments, or obvious references.
- 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. The total length should not exceed 18 pages.
- 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) or PostScript (a .ps file) format.
- If at all possible, the paper should use Type 1 (outline) fonts rather than Type 3 (bitmap) fonts.

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 workshop.

Program Committee

- Amr Youssef, Concordia University, Canada
- Andrey Bogdanov, K.U. Leuven, Belgium
- Anne Canteaut, INRIA, France and Technical University of Denmark
- Anwar Hasan, University of Waterloo, Canada
- Arash Reyhani-Masoleh, University of Western Ontario, Canada
- Bart Preneel, K.U. Leuven, Belgium
- Carlisle Adams, University of Ottawa, Canada
- Gaetan Leurent, University of Luxembourg
- Gregor Leander, Technical University of Denmark
- Guang Gong, University of Waterloo, Canada
- Huapeng Wu, University of Windsor, Canada (Co-chair)
- Jean-Philippe Aumasson, NAGRA, Switzerland
- Joan Daemen, ST Microelectronics, Belgium
- Kaisa Nyberg, Aalto University, Finland
- Keith Martin, University of London - Royal Holloway, UK
- Lars R. Knudsen, Technical University of Denmark (Co-chair)
- María Naya-Plasencia, University of Versailles, France
- Martijn Stam, University of Bristol, UK
- Martin Hell, Lund University, Sweden
- Martin Schläffer, TU Graz, Austria
- Matt Robshaw, Orange, France
- Ruizhong Wei, Lakehead University, Canada
- Svetla Nikova, University of Twente, The Netherlands
- Taizo Shirai, Sony Corporation, Japan
- Ted Krovetz, California State University, USA
- Vassil Dimitrov, University of Calgary, Canada
- Yu Sasaki, NTT, Japan