SAC 2010 Call for Papers

August 12-13, 2010
Waterloo, Ontario, Canada
http://sac2010.uwaterloo.ca/

The Workshop on Selected Areas in Cryptography (SAC) is an annual conference dedicated to specific themes in the area of cryptographic system design and analysis. SAC 2010 will take place on August 12-13, 2010, at the University of Waterloo, in Ontario, Canada.

Authors are encouraged to submit original papers related to the themes for the SAC 2010 workshop:

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. Applications of coding theory and combinatorics in cryptography.

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 workshop record will be available to participants during the workshop. Instructions about the preparation of a final proceedings version will be sent to the authors of accepted papers.

Important dates

Submission deadline	May 17, 2010
Notification of decision	July 6, 2010
Preproceedings version deadline	July 20, 2010
Workshop	August 12-13, 2010

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 (http://www.springer.de/comp/lncs, 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 unable to submit electronically or who cannot use LaTeX should contact the co-chairs by April 30, 2010. Authors of accepted papers must guarantee that their paper will be presented at the workshop.

Stipends

A limited number of stipends are available to those unable to obtain funding to attend the workshop. Students, whose papers are accepted and who will present the paper themselves are encouraged to apply if such assistance is needed. Requests for stipends should be addressed to Guang Gong.

Organizing Committee

Alex Biryukov	University of Luxembourg
Guang Gong	University of Waterloo
Douglas Stinson	University of Waterloo

Program Committee

Roberto Avanzi	Ruhr-University Bochum
Paulo Barreto	University of Sao Paulo, Brazil
Simon Blackburn	Royal Holloway, University of London, U.K.
Christophe De Cannière	Katholieke Universiteit Leuven, Belgium
Anne Canteaut	INRIA, France
Joan Daemen	ST Microelectronics, Belgium
Orr Dunkelman	Weizmann Institute of Science, Israel
Henri Gilbert	Orange Labs, France
Helena Handschuh	Katholieke Universiteit Leuven, Belgium
Martin Hell	Lund University, Sweden
Howard Heys	Memorial University, Canada
Tetsu Iwata	Nagoya University, Japan
Mike Jacobson	University of Calgary, Canada
David Jao	University of Waterloo, Canada
Marc Joye	Thomson R&D, France
Tanja Lange	Technische Universiteit Eindhoven, Netherlands

Barbara Masucci	Università di Salerno, Italy
Ali Miri	Ryerson University and University of Ottawa
Ilya Mironov	Microsoft Research, USA
David Naccache	ENS, France
Kaisa Nyberg	Helsinki University of Technology and NOKIA, Finland
Carles Padró	Universitat Politècnica de Catalunya, Spain
Maura Paterson	Birkbeck, University of London, U.K.
Svetla Petkova-Nikova	K.U. Leuven Belgium and Univeristy of Twente, Netherlands
Bart Preneel	Katholieke Universiteit Leuven, Belgium
Christian Rechberger	Katholieke Universiteit Leuven, Belgium
Thomas Ristenpart	UC San Diego, USA
Rei Safavi-Naini	University of Calgary, Canada
Yu Sasaki	NTT, Japan
Martijn Stam	EPFL, Switzerland
Francois-Xavier Standaert	Université Catholique de Louvain, Belgium
Tamir Tassa	The Open University, Israel
Nicolas Theriault	Universidad de Talca, Chile
Serge Vaudenay	EPFL, Switzerland
Ruizhong Wei	Lakehead University, Canada
Amr Youssef	Concordia University, Canada
Gilles Zemor	Université Bordeaux, France