Call for Papers

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. Authors are encouraged to submit original papers related to the themes for the SAC 2007 workshop:

- Design and analysis of symmetric key cryptosystems
- Primitives for symmetric key cryptography, including block and stream ciphers, hash functions, and MAC algorithms
- Efficient implementations of symmetric and public key algorithms
- Innovative cryptographic defenses against malicious software

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.

Submission Format

- 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 20 pages.
- The submission 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.
- We recommend that the paper be typeset using LaTeX and the LNCS style available at http://www.springer.de/comp/lncs. Submissions should be in PDF (i.e., a .pdf file), or PostScript (i.e., a .ps file) format.
- If at all possible, the paper should use Type 1 fonts (rather than Type 3 fonts).
- Papers must be submitted electronically by ~~May 11, 2007~~ **(now May 18, 2007)**, 12:00 EST. A detailed description of the electronic submission procedure can be found at https://punchscan.org/~aleks/sac2007/submit/ (Note that this server uses a self-signed certificate for its SSL connection, so please take appropriate steps to deal with any warning messages that your browser may display.)

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 20, 2007.

Conference Proceedings

The proceedings will be published in Springer-Verlag's Lecture Notes in Computer Science (LNCS) Series (http://www.springer.de/comp/lncs/index.html). 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. Authors of an accepted paper must guarantee that at least one of the authors will attend the workshop and present their paper, and that the final paper will be typeset in LaTeX.

Important Dates

- Paper Submission Deadline: ~~May 11, 2007~~ at 12:00 EST **(now May 18, 2007)**
- Notification of Acceptance: June 22, 2007
- Pre-Proceedings Papers Deadline: July 13, 2007
- Workshop Event: August 16 & 17, 2007
- Proceedings Version Deadline: September 14, 2007

Contact Information

This year's workshop is co-chaired by Carlisle Adams, Ali Miri, and Michael Wiener. Questions regarding the workshop should be sent to <sac2007 (at) site.uottawa.ca> or directly to one of the co-chairs.

Carlisle Adams
University of Ottawa
800 King Edward Avenue
Ottawa, Ontario, Canada
K1N 6N5
phone: (613) 562-5800 ext. 2345
email: cadams (at) site dot uottawa dot ca

Ali Miri
University of Ottawa
161 Louis Pasteur
Ottawa, Ontario, Canada
K1N 6N5
phone: (613) 562-5800 ext. 6111
email: samiri (at) site dot uottawa dot ca

Michael Wiener
Cryptographic Clarity
20 Hennepin St.
Nepean, Ontario, Canada
K2J 3Z4
phone: (613) 825-8496
email: michael.wiener (at) sympatico dot ca

Program Committee

Carlisle Adams (co-chair), University of Ottawa, Canada
Roberto Avanzi, Ruhr-University Bochum, Germany
Orr Dunkelman, Katholieke Universiteit Leuven, Belgium
Ian Goldberg, University of Waterloo, Canada
Helena Handschuh, Spansion, France
M. Anwar Hasan, University of Waterloo, Canada
Antoine Joux, DGA and Université de Versailles St-Quentin-en-Yvelines, France
Pascal Junod, Nagravision, Switzerland
Tanja Lange, Technische Universiteit, Eindhoven, Netherlands
Arjen Lenstra, EPFL, Switzerland
Ali Miri (co-chair), University of Ottawa, Canada
Christof Paar, Ruhr-University Bochum, Germany
Bart Preneel, Katholieke Universiteit Leuven, Belgium
Vincent Rijmen, Graz University of Technology, Austria
Matt Robshaw, France Telecom, France
Greg Rose, QUALCOMM, USA
Doug Stinson, University of Waterloo, Canada
Serge Vaudenay, EPFL, Switzerland
Michael Wiener (co-chair), Cryptographic Clarity, Canada
Robert Zuccherato, Entrust Inc., Canada

Travel Support

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 the workshop co-chairs.

Previous SAC Workshops

Information about previous SAC Workshops can be found at
http://www.cacr.math.uwaterloo.ca/~dstinson/SAC/SACworkshops.html