SAC 2004

11th Annual Workshop on
Selected Areas in Cryptography
Aug 9 & 10, 2004, Waterloo, Ontario, Canada

`http://vlsi.uwaterloo.ca/~sac04`

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 2004 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
- Cryptographic solutions for mobile (web) services

Submissions must not substantially duplicate work that any of the authors has published elsewhere or has submitted in parallel to any other conference or workshop that has proceedings. Papers must be submitted electronically. Detailed description of the electronic submission procedure is available at `https://silentbob.gemplus.com/sac2004/submit/`. Submissions must conform to this procedure. We recommend that the PS or PDF file of each paper be generated using LaTeX and the LNCS style available at `http://www.springer.de/comp/lncs`. The submission must not exceed 15 pages in total using the font sizes and margins of the LNCS style. Submissions not meeting these guidelines risk rejection without consideration of their merits.

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.

Important Dates

Paper Submission Deadline	May 7, 2004
Notification of Acceptance	June 21, 2004
Pre-Proceedings Version of Papers Deadline	July 12, 2004
Workshop	August 9 and 10, 2004
Proceedings Version Deadline	September 9, 2004

Program Committee

Carlisle Adams, University of Ottawa, Canada
Henri Gilbert, France Telecom, France
Helena Handschuh, Gemplus, France (Co-chair)
Anwar Hasan, University of Waterloo, Canada (Co-chair)
Mike Just, Carleton University, Canada
Charanjit Jutla, IBM, USA
Arjen Lenstra, Citibank, USA and Technische Universiteit Eindhoven, The Netherlands
Stefan Lucks, Universität Mannheim, Germany
Mitsuru Matsui, Mitsubishi Electric, Japan
Alfred Menezes, University of Waterloo, Canada
Shiho Moriai, Sony Computer Entertainment Inc., Japan
Kaisa Nyberg, Nokia, Finland
Bart Preneel, Katholieke Universiteit Leuven, Belgium
Matt Robshaw, Royal Holloway University of London, U.K.
Doug Stinson, University of Waterloo, Canada
Serge Vaudenay, EPFL, Switzerland
Michael Wiener, Cryptographic Clarity, Canada

Contact Information

This year's workshop is co-chaired by Helena Handschuh of Gemplus, France and Anwar Hasan of University of Waterloo, Canada. Questions regarding the workshop should be sent to `sac04@ece.uwaterloo.ca` or directly to one of the co-chairs.

Helena Handschuh
Security Technologies Department
Gemplus R&D
34, rue Guynemer
92447 Issy-les-Moulineaux Cedex
France
Tel: +33 (0)1 46 48 20 37
Fax: +33 (0)1 46 48 20 04
Email: `Helena.HANDSCHUH@gemplus.com`

Anwar Hasan
Dept. of Electrical & Computer Eng.
University of Waterloo
200 Univ. Ave. West
Waterloo, Ontario, N2L 3G1
Canada
Tel: +1 519 888 4567 ext. 2868
Fax: +1 519 746 3077
Email: `ahasan@ece.uwaterloo.ca`

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.

Further Information

Please visit the workshop website at `http://vlsi.uwaterloo.ca/~sac04/`