Conference Information:

The 15th annual Fast Software Encryption workshop, sponsored by the International Association for Cryptologic Research (IACR), invites original research papers on symmetric cryptology. The workshop focuses on fast and secure primitives for symmetric cryptography, including the design and analysis of block ciphers, stream ciphers, encryption schemes, analysis and evaluation tools, hash functions, and message authentication codes (MACs).

Instructions for Authors:

Submissions must not substantially duplicate work that any of the authors has published in a journal or a conference/workshop with proceedings, or has submitted/is planning to submit before the author notification deadline to a journal or other conferences/workshops that have proceedings. Accepted submissions may not appear in any other conference or workshop that has proceedings. Double submissions will be rejected without evaluation; see IACR Policy on Irregular Submissions.

Submissions must be anonymous, with no author names, affiliations, acknowledgments, or obvious references. It should begin with a title, a short abstract, and a list of keywords. The length of the submission should be at most 14 pages excluding bibliography and appendices using at least 11pt size font, reasonably sized margins and in total not more than 20 pages. 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. Submissions not meeting these guidelines risk rejection without consideration of their merits.

It is strongly preferred that submissions be processed in LaTeX according to the instructions listed on http://www.springer.de/comp/lncs/authors.html since these are mandatory for the final papers. Submitted papers must be in PDF or postscript format and should be submitted electronically. Detailed description of the electronic submission procedure will be available via http://fse2008.epfl.ch.

Authors of accepted papers must guarantee that their paper will be presented at the workshop.

Proceedings:

Pre-proceedings will be available at the workshop. Proceedings are intended to be published in Springer-Verlag’s Lecture Notes in Computer Science series. Authors of accepted papers will be required to complete the IACR copyright assignment form at http://www.iacr.org/forms/copyright_agreement.html for their work to be published in the workshop proceedings.

Workshop Information and Stipends:

The primary source of information is http://fse2008.epfl.ch. 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 sent to Thomas Baignères.

Program Committee:

Frederik Armknecht Ruhr-University Bochum, Germany
Steve Babbage Vodafone, U.K.
Alex Biryukov University of Luxembourg, Luxembourg
John Black University of Colorado, USA
Anne Canteaut INRIA, France
Claude Carlet University of Paris 8, France
Joan Daemen STMicroelectronics, Belgium
Orr Dunkelman K.U.Leuven, Belgium
Henri Gilbert France Telecom, France
Louis Granboulan EADS, France
Helena Handschuh Spanvision, France
Tetsu Iwata Nagoya University, Japan
Thomas Johansson Lund University, Sweden
Antoine Joux DGA and University of Versailles, France
Pascal Junod Nagravision, Switzerland
Charanjit Jutla IBM Watson, U.S.A.
Mitsuru Matsui Mitsubishi Electric, Japan
Willi Meier FHNW, Switzerland
Kaisa Nyberg (chair) Helsinki University of Technology and NOKIA, Finland
Elisabeth Oswald University of Bristol, U.K.
Josef Pieprzyk Macquarie University, Australia
Bart Preneel K.U.Leuven, Belgium
Vincent Rijmen Graz University of Technology, Austria
Greg Rose Qualcomm, U.S.A.

Program Chair:

Kaisa Nyberg
Helsinki University of Technology
Department of Computer Science and Engineering
Laboratory for Theoretical Computer Science
P.O. Box 5400, FI-02015 TKK
Finland
email: Kaisa.Nyberg@tkk.fi

General co-Chairs:

Thomas Baignères and Serge Vaudenay
Ecole Polytechnique Fédérale de Lausanne
I&C - Security and Cryptography Laboratory
INF 241 (INF Building), Station 14
CH-1015 Lausanne
Switzerland
email: Thomas.Baigneres(at)epfl.ch
Serge.Vaudenay(at)epfl.ch