

Fast Software Encryption 2009

Call For Papers

<https://www.cosic.esat.kuleuven.be/fse2009/>



FSE 2009 is the 16th annual Fast Software Encryption workshop, for the seventh year sponsored by the International Association for Cryptologic Research (IACR). FSE 2009 will take place in Leuven, Belgium and will be followed by NIST's first hash function candidate conference. Original research papers on symmetric cryptology are invited for submission to FSE 2009. The workshop concentrates 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).

Important dates

Submission deadline:	November 24, 2008
Notification of decision:	January 20, 2009
Pre-proceedings version deadline:	February 10, 2009
Workshop:	February 22 – 25, 2009
Proceedings version deadline:	April 1, 2009

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 for further details.

The submission 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 single column with 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. New proposals should be accompanied with test vectors and analysis. 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. A detailed description of the electronic submission procedure will be available via <https://www.cosic.esat.kuleuven.be/fse2009/>.

The authors of submitted papers guarantee that their paper will be presented at the workshop if their paper is accepted.

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.

Program Committee

Steve Babbage	Vodafone Group R&D, UK
Alex Biryukov	University of Luxembourg, Luxembourg
Dan J. Bernstein	University of Illinois at Chicago, USA
Joan Daemen	STMicroelectronics, Belgium
Christophe De Cannière	Ecole Normale Supérieure, France and Katholieke Universiteit Leuven, Belgium
Orr Dunkelman (chair)	Ecole Normale Supérieure, France
Henri Gilbert	Orange Labs, France
Louis Granboulan	EADS Innovation Works, France
Helena Handschuh	Spansion, France
Tetsu Iwata	Nagoya University, Japan
Nathan Keller	Hebrew University, Israel
Stefan Lucks	Bauhaus-University Weimar, Germany
Mitsuru Matsui	Mitsubishi Electric, Japan
Willi Meier	FHNW, Switzerland
Kaisa Nyberg	Helsinki University of Technology and NOKIA, Finland
Raphael Phan	Loughborough University, UK
Bart Preneel	Katholieke Universiteit Leuven, Belgium
Håvard Raddum	University of Bergen, Norway
Christian Rechberger	Graz University of Technology, Austria
Thomas Ristenpart	UC San Diego, USA
Greg Rose	Qualcomm, Australia
Serge Vaudenay	EPFL, Switzerland
Yiqun Lisa Yin	Independent Consultant, USA

Workshop Information and Stipends

The primary source of information is <https://www.cosic.esat.kuleuven.be/fse2009/>. 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 fse2009@esat.kuleuven.be.