Call for Papers

FSE 2007 is the 14th annual Fast Software Encryption workshop, for the sixth year sponsored by the International Association for Cryptologic Research (IACR). Original research papers on symmetric cryptology are invited for submission to FSE 2007. The workshop concentrates on fast and secure primitives for symmetric cryptography, including the design and analysis of block ciphers, stream ciphers, encryption schemes, hash functions, and message authentication codes (MACs), analysis and evaluation tools.

Important dates

Submission deadline: December 11, 2006
Notification of decision: January 31, 2007
Pre-proceedings version deadline: February 20, 2007
Workshop: March 26 - 28, 2007
Proceedings version deadline: April 25, 2007

Instructions for Authors

Submissions must not substantially duplicate work that any of the authors has published elsewhere or has submitted in parallel to any other international conference or workshop that has proceedings. Double submissions will be rejected without evaluation.

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 12 pages excluding bibliography and appendices using at least 11pt size font, reasonably sized margins and total of 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](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://lacs.uni.lu/fse2007/](http://lacs.uni.lu/fse2007/).

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](http://www.iacr.org/forms/copyright_agreement.html) for their work to be published in the workshop proceedings.

**Program Committee**

Frederik Armknecht  NEC, Germany  
Steve Babbage  Vodafone, U.K.  
Alex Biryukov (chair)  University of Luxembourg, Luxembourg  
Claude Carlet  INRIA+University of Paris 8, France  
Nicolas Courtois  Gemalto, France  
Joan Daemen  STMicroelectronics, Belgium  
Orr Dunkelman  K.U.Leuven, Belgium  
Henri Gilbert  France Telecom, France  
Louis Granboulan  EADS, France  
Helena Handschuh  Spansion, France  
Jin Hong  Seoul National University, Korea  
Seokhie Hong  CIST, Korea  
Tetsu Iwata  Nagoya University, Japan  
Thomas Johansson  Lund University, Sweden  
Antoine Joux  DGA + University of Versailles, France  
Pascal Junod  Nagravision, Switzerland  
Charanjit Jutla  IBM Watson, U.S.A.  
John Kelsey  NIST, U.S.A.  
Lars R. Knudsen  Technical University of Denmark, Denmark
Workshop Information and Stipends

The primary source of information is http://lacs.uni.lu/fse2007/ but any remaining questions can be sent to fse2007@uni.lu. 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 fse2007@uni.lu.