Call for Papers

FSE 2005 is the 12th annual Fast Software Encryption workshop, sponsored by the International Association for Cryptologic Research for the fourth year. Original research papers on symmetric cryptology are invited for submission to FSE 2005. The workshop concentrates on all aspects of fast primitives for symmetric cryptography: the design and cryptanalysis of block and stream ciphers, as well as hash functions and message authentication codes (MACs).

Important dates

<table>
<thead>
<tr>
<th>Event</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Workshop</td>
<td>February 21-23, 2005</td>
</tr>
<tr>
<td>Submission deadline</td>
<td>November 19, 2004</td>
</tr>
<tr>
<td>Notification of decision</td>
<td>January 10, 2005</td>
</tr>
<tr>
<td>Pre-proceedings version deadline</td>
<td>January 28, 2005</td>
</tr>
<tr>
<td>Proceedings version deadline</td>
<td>March 31, 2005</td>
</tr>
</tbody>
</table>

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. It 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. It should have reasonable sized margins. 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 Li\TeX{} according to the instructions listed on [http://www.springer.de/comp/lncs/authors.html](http://www.springer.de/comp/lncs/authors.html) since this will be a mandatory requirement for the final papers.

Submission deadline: November 19, 2004. Notification of acceptance will be sent to authors by January 10, 2005. Authors of accepted papers must guarantee that their paper will be presented at the workshop. Submitted papers must be in PDF or PostScript format and should be submitted electronically. Detailed description of the electronic submission procedure will be available here: [https://silentbob.gemplus.com/fse2005/submit/](https://silentbob.gemplus.com/fse2005/submit/)
Proceedings

Pre-proceedings will be available at the workshop. Proceedings are intended to be published in Springer-Verlag's Lecture Notes in Computer Science (LNCS) series. Instructions about the preparation of a final proceedings version will be sent to the authors of accepted papers after the workshop.

Program Committee

Kazumaro Aoki
Steve Babbage
Eli Biham
Anne Canteaut
Don Coppersmith
Joan Daemen
Henri Gilbert (co-chair)
Helena Handschuh (co-chair)
Thomas Johansson
Antoine Joux
Xuejia Lai
Stefan Lucks
Mitsuru Matsui
Willi Meier
Kaisa Nyberg
Bart Preneel
Matt Robshaw
Palash Sarkar
Serge Vaudenay
Moti Yung

NTT, Japan
Vodafone, UK
Technion, Israel
INRIA, France
IBM Research, USA
STMicroelectronics, Belgium
France Telecom R&D, France
Gemplus, France
Lund University, Sweden
France
Shanghai Jiaotong University, China
Univ. Mannheim, Germany
Mitsubishi Electric, Japan
FH Aargau, Switzerland
Nokia, Finland
K.U.Leuven, Belgium
Royal Holloway, University of London, UK
Indian Statistical Institute, India
EPFL, Switzerland
Columbia University, USA

Workshop information

Further information is available on the FSE 2005 web-page:

http://crypto.rd.francetelecom.com/fse2005/

For any additional information, please contact one of the co-chairs:

Helena Handschuh, helena.handschuh@gemplus.com
Henri Gilbert, henri.gilbert@francetelecom.com

Stipends

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 one of the co-chairs.