FSE 2012
Call for Papers

March 19–21, 2012, Washington DC, USA
http://fse2012.inria.fr/

Submission deadline	November 17, 2011 (11:59 UTC)
Notification of decision	January 23, 2012
Preproceedings version deadline	February 13, 2012
Workshop	March 19–21, 2012
Proceedings version deadline	April 30, 2012

General Information

FSE 2012 is the 19th annual Fast Software Encryption workshop, for the eleventh year sponsored by the International Association for Cryptologic Research (IACR). FSE 2012 will take place in Washington DC, USA. Original research papers on symmetric cryptology are invited for submission to FSE 2012. 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).

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. IACR reserves the right to share information about submissions with other program committees to detect parallel submissions and the IACR policy[1] on irregular submissions will be strictly enforced. Double submissions with the co-located third SHA-3 conference[2] are allowed, but the papers accepted for FSE 2012 will be presented at FSE 2012 only, in order to avoid double presentations.

The submission must be written in English and 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. 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.

Submissions to FSE 2012 should be submitted electronically in PDF format. A detailed description of the electronic submission procedure will be available on FSE 2012 website.

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

Proceedings

Preproceedings will be available at the workshop. Proceedings will 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, as available on the IACR website[3], for their work to be published in the workshop final proceedings.

[1] See http://www.iacr.org/docs/irregular.pdf for further details.
[2] http://csrc.nist.gov/groups/ST/hash/sha-3/Round3/March2012/.
[3] See http://www.iacr.org/forms/copyright_agreement.html

Workshop Information and Stipends

The primary source of information is the workshop website `http://fse2012.inria.fr/`. 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 the general chair.

Program Committee

Alex Biryukov	*University of Luxembourg, Luxembourg*
Anne Canteaut (Chair)	*INRIA Paris-Rocquencourt, France*
Guang Gong	*University of Waterloo, Canada*
Martin Hell	*Lund University, Sweden*
Antoine Joux	*DGA and Université de Versailles Saint-Quentin-en-Yvelines, France*
Pascal Junod	*HEIG-VD, Switzerland*
John Kelsey	*NIST, USA*
Dmitry Khovratovich	*Microsoft Research, USA*
Lars Ramkilde Knudsen	*Technical University of Denmark, Denmark*
Gregor Leander	*Technical University of Denmark, Denmark*
Stefan Lucks	*Bauhaus-Universität Weimar, Germany*
Subhamoy Maitra	*ISI Kolkata, India*
Willi Meier	*FHNW, Switzerland*
Shiho Moriai	*Sony Corporation, Japan*
María Naya-Plasencia	*FHNW, Switzerland*
Elisabeth Oswald	*University of Bristol, United Kingdom*
Vincent Rijmen	*K.U.Leuven, Belgium and TU Graz, Austria*
Matt Robshaw	*Orange Labs, France*
Yu Sasaki	*NTT Corporation, Japan*
François-Xavier Standaert	*Université catholique de Louvain, Belgium*
Serge Vaudenay	*EPFL, Switzerland*
Gilles Van Assche	*STMicroelectronics, Belgium*

General Chair

Bruce Schneier	*British Telecom, USA*

Contact Information

All correspondence and/or questions should be directed to:

Bruce Schneier	Anne Canteaut
British Telecom, USA	INRIA Paris-Rocquencourt, France
`schneier@schneier.com`	`anne.canteaut@inria.fr`

Recommended Submission Style

Electronic submissions to FSE 2012 should be in Portable Document Format (PDF). The submission should preferably be in A4 paper size and use Type 1 fonts (rather than Type 3 fonts which usually look fuzzy and ugly when viewed on screen).

The following procedure is recommended for generating submissions.

Preparing the LaTeX file. To get 11 point fonts, reasonable margins and A4 paper, you obtain the `llncs` package and use the following two lines of the beginning of your LaTeX file:

```
\documentclass[11pt]{llncs}
\usepackage[a4paper,hmargin=2.5cm,vmargin=3cm]{geometry}
```

You should not use any other command to set the margin and/or change the font. This LaTeX style will be used for the preproceedings.

Generating PDF file with `pdflatex`. After using the above declaration, assuming that your paper is stored in the file `paper.tex`, it suffices to type the command:

```
$ pdflatex paper
```

This generates a file `paper.pdf` ready for submission. There are other, more complex, procedures to generate such PDF files. These alternative procedures are not recommended. If, for some reason, an alternative procedure is used, the resulting PDF file should be verified using the following commands:

```
$ pdfinfo paper.pdf
$ pdffonts paper.pdf
```

These two commands respectively print general information (including paper size) and font information.

Including graphics. To insert graphics into your PDF file, there are two different options:

- ➢ Generate the graphics using a text description within LaTeX.
- ➢ Include an externally generated graphics file.

➢ For the first option, authors should consider the PGF package. It can be used by including the following line in the LaTeX file:

```
\usepackage{pgf}
```

The PGF package also offer several options for drawing arrows, diagrams and shadings. To use these options, replace the above line by:

```
\usepackage{pgf,pgfarrows,pgfnodes,pgfshade}
```

➢ To use externally generated graphics, a convenient method relies on the following package:

```
\usepackage{graphicx,color}
```

With this package, a PDF file `drawing.pdf` can be included using:

```
\includegraphics{drawing}
```

Authors should make sure that their externally generated graphics PDF files have a correct bounding box specification.