FSE 2014
Call for Papers

March 3–5, 2014, London – UK
http://fse2014.isg.rhul.ac.uk/

Submission deadline	November 12, 2013 (23:59 UTC)
Notification of decision	January 18, 2014
Preproceedings version deadline	February 13, 2014
Workshop	March 3–5, 2014
Proceedings version deadline	April 30, 2014

General Information

FSE 2014 is the 21st edition of Fast Software Encryption workshop, and one of the International Association for Cryptologic Research (IACR) flagship annual events. FSE 2014 will take place in London, on March 3–5, 2014. Original research papers on symmetric cryptology are invited for submission to FSE 2014. 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, (cryptographic) permutations, authenticated encryption schemes, and analysis and evaluation tools.

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.

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 final version of accepted papers will have to follow the LNCS guidelines (`http://www.springer.com/computer/lncs`) using Springer's standard fonts, font sizes, and margins with a total page limit of 20 pages including references and appendices. **Submissions to FSE 2014 should follow the same format.**

A submission may include additional supporting information beyond the 20-page LNCS limit. If authors believe that more details are essential to substantiate the claims of their paper, they are encouraged to use this space to include proofs, source code, and other information allowing verification of results; unverifiable papers risk rejection. However, committee members will read any additional supporting information provided at their discretion, so the submission should be intelligible and self-contained within 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 2014 should be submitted electronically in PDF format. A detailed description of the electronic submission procedure will be available on the FSE 2014 website. The authors of submitted papers guarantee that their paper will be presented at the workshop if it is accepted. A preliminary list of accepted papers, not including conditional accepts, will be published immediately after the decision is finalized, with the information supplied by the authors at submission time.

Proceedings

Preproceedings will be available at the workshop in electronic form. 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[2], for their work to be published in the workshop final proceedings.

[1] See `http://www.iacr.org/docs/irregular.pdf` for further details.
[2] See `http://www.iacr.org/docs/copyright_form.pdf`

Workshop Information and Stipends

The primary source of information is the workshop website `http://fse2014.isg.rhul.ac.uk/`. 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 chairs.

Program Committee

Martin Albrecht	*Technical University of Denmark, Denmark*
Elena Andreeva	*KU Leuven, Belgium*
Kazumaro Aoki	*NTT, Japan*
Frederik Armknecht	*University of Mannheim, Germany*
Daniel J. Bernstein	*University of Illinois at Chicago, USA, and Technische Universiteit Eindhoven, Netherlands*
John Black	*University of Colorado at Boulder, USA*
Anne Canteaut	*Inria Paris-Rocquencourt, France*
Carlos Cid (Co-chair)	*Royal Holloway University of London, UK*
Joan Daemen	*STMicroelectronics, Belgium*
Christophe De Cannière	*Google, Switzerland*
Orr Dunkelman	*University of Haifa, Israel*
Martin Hell	*Lund University, Sweden*
Dmitry Khovratovich	*University of Luxembourg, Luxembourg*
Gregor Leander	*RU Bochum, Germany*
Subhamoy Maitra	*ISI Kolkata, India*
Mitsuru Matsui	*Mitsubishi Electric, Japan*
Florian Mendel	*TU Graz, Austria*
Svetla Nikova	*KU Leuven, Belgium*
Elisabeth Oswald	*University of Bristol, United Kingdom*
Thomas Peyrin	*Nanyang Technological University, Singapore*
Josef Pieprzyk	*Macquarie University, Australia*
Christian Rechberger (Co-chair)	*Technical University of Denmark, Denmark*
Martijn Stam	*University of Bristol, United Kingdom*
François-Xavier Standaert	*Université catholique de Louvain, Belgium*
Serge Vaudenay	*EPFL, Switzerland*
Hongbo Yu	*Tsinghua Univeristy, China*

General Chairs and Contact Information

All correspondence and/or questions should be sent to `fse2014@rhul.ac.uk`

Carlos Cid
Royal Holloway, University of London
Egham, TW20 0EX
United Kingdon

Christian Rechberger
DTU – Technical University of Denmark
DK-2800 Lyngby
Denmark

Instructions on Submission Style

Electronic submissions to FSE 2014 should be in Portable Document Format (PDF). The submission should follow the LNCS guidelines (`http://www.springeronline.com/lncs`), using Springer's standard fonts, font size (10pt) and margins, with a total page limit of 20 pages including references and appendices.

The following procedure is recommended for generating submissions.

Preparing the LaTeX file. You should obtain the `llncs` package and start your LaTeX file with the following line:

```
\documentclass{llncs}
```

You should not use any other command to set the margin and/or change the font. This will ensure your submission will use LNCS standard margins and font sizes. This LaTeX style will be used for both the preproceedings and the workshop proceedings.

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.