FSE 2015
Call for Papers

March 8–11, 2015, Istanbul, Turkey
`http://light-sec.org/fse2015/`

Submission deadline	November 7, 2014 (11:59 AM UTC)
Notification of decision	January 16, 2015
Preproceedings version deadline	February 13, 2015
Workshop	March 8–11, 2015
Proceedings version deadline	April 30, 2015

General Information

FSE 2015 is the 22nd edition of Fast Software Encryption workshop, and one of the International Association for Cryptologic Research (IACR) flagship annual events. FSE 2015 will take place in Istanbul, on March 8-11, 2015. Original research papers on symmetric cryptology are invited for submission to FSE 2015. 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 (`http://www.iacr.org/docs/irregular.pdf`) 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 introduction should summarize the contributions of the paper at a level appropriate for a non-specialist reader. 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 (see last section below for details). **Submissions to FSE 2015 should follow the same format.** A submission may include (clearly marked) 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.

Submissions not meeting these guidelines risk rejection without consideration of their merits.

Submissions to FSE 2015 must be submitted electronically in PDF format. A detailed description of the electronic submission procedure will be available on FSE 2015 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[1], for their work to be published in the workshop final proceedings.

Workshop Information and Stipends

The primary source of information is the workshop website. 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

Elena Andreeva	*KU Leuven, Belgium*
Kazumaro Aoki	*NTT Secure Platform Laboratories, Japan*
Daniel Bernstein	*University of Illinois at Chicago, USA, and TU/e, Netherlands*
Céline Blondeau	*Aalto University, Finland*
Andrey Bogdanov	*Technical University Denmark, Denmark*
Anne Canteaut	*Inria, France*
Joan Daemen	*STMicroelectronics, Belgium*
Itai Dinur	*Ecole Normale Superieure, Paris, France*
Orr Dunkelman	*University of Haifa, Israel*
Tetsu Iwata	*Nagoya University, Japan*
Orhun Kara	*TUBITAK - BILGEM, Turkey*
Dmitry Khovratovich	*University of Luxembourg, Luxembourg*
Gregor Leander (Chair)	*HGI, Ruhr University Bochum, Germany*
Gaëtan Leurent	*Inria, France*
Stefan Lucks	*Bauhaus-Universität Weimar, Germany*
Amir Moradi	*HGI, Ruhr University Bochum, Germany*
María Naya-Plasencia	*Inria, France*
Svetla Nikova	*KU Leuven, Belgium*
Thomas Peyrin	*Nanyang Technological University, Singapore*
Vincent Rijmen	*KU Leuven, Belgium*
Martin Schlaeffer	*Infineon Technologies, Austria*
Tom Shrimpton	*Portland State University, USA*
Martijn Stam	*University of Bristol, United Kingdom*
François-Xavier Standaert	*Universite catholique de Louvain, Belgium*
Vesselin Velichkov	*University of Luxembourg, Luxembourg*
Tolga Yalcin	*UIST St Paul the Apostle, Macedonia*

General Chair

Hüseyin Demirci	*TUBITAK - BILGEM, Turkey*

[1] See `http://www.iacr.org/forms/copyright_agreement.html`

Contact Information

All correspondence and/or questions should be directed to:

Hüseyin Demirci
TUBITAK - BILGEM, Turkey
huseyin.demirci@tubitak.gov.tr

Gregor Leander
HGI, Ruhr University Bochum, Germany
fse2015programchair@iacr.org

Recommended Submission Style

Electronic submissions to FSE 2015 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 follow the standard LNCS guidelines, you obtain the `llncs` package and use the following line at the beginning of your LaTeX file:

```
\documentclass{llncs}
```

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.