Fast Software Encryption 2018
IACR Transactions on Symmetric Cryptology

Call for Papers

General Information on FSE 2018

25th International Conference Fast Software Encryption (FSE 2018)
Bruges, Belgium
March 5-7, 2018
General information: `https://fse.iacr.org/2018/`
Submission server: `http://tosc.iacr.org/index.php/ToSC/pages/view/Submission`

FSE 2018 is the 25th edition of Fast Software Encryption conference, and one of the conferences organized by the International Association for Cryptologic Research (IACR). FSE 2018 will take place in Bruges, on March 5-7, 2018. Original research papers on symmetric cryptology are invited for submission to FSE 2018. The scope of FSE concentrates on fast and secure primitives for symmetric cryptography, including the design and analysis of block ciphers, stream ciphers, encryption schemes, hash functions, message authentication codes, (cryptographic) permutations, authenticated encryption schemes, cryptanalysis and evaluation tools, and security issues and solutions regarding their implementation. Since last year, FSE 2018 also solicits submissions for **Systematization of Knowledge** (SoK) papers. These papers aim at reviewing and contextualizing the existing literature in a particular area in order to systematize the existing knowledge in that area. To be considered for publication, they must provide an added value beyond prior work, such as novel insights or reasonably questioning previous assumptions.

Publication Model

From last year, FSE has moved to an open-access journal/conference hybrid model. Submitted articles undergo a journal-style reviewing process. Accepted papers are published in **Gold Open Access** (free availability from day one) by the Ruhr University of Bochum in an issue of the newly established journal **IACR Transactions on Symmetric Cryptology**.
The yearly FSE event will consist of presentations of the articles accepted to the journal IACR Transactions on Symmetric Cryptology, as well as invited talks and social activities. This new model has been established as a way to improve reviewing and publication quality while retaining the highly successful community event FSE. For any further information, please view the FAQ page: `http://tosc.iacr.org/index.php/ToSC/pages/view/FAQ`
For FSE 2018, authors can submit papers to the IACR Transactions on Symmetric Cryptology four times, every three months on a predictable schedule. Authors are notified of the decisions about two months after submission. In addition to accept and reject decisions, papers may be provided with **"minor revision"** decisions, in which case the paper is conditionally accepted and an assigned shepherd will verify if the

changes are applied, or **"major revision"** decisions, in which case authors are invited to revise and resubmit their article to one of the following two submission deadlines, otherwise the paper will be treated as a new submission. We endeavor to assign the same reviewers to revised versions.
Papers accepted for publication before the end of January 2018 will be presented at that year's conference. Note that it is **mandatory that accepted papers at the IACR Transactions on Symmetric Cryptology journal are presented at the corresponding FSE event**.

Timeline for FSE 2018 / IACR Transactions on Symmetric Cryptology 2017/2018

All upcoming deadlines are 23:59:59 Greenwich Mean Time (UTC)

Volume IACR Transactions on Symmetric Cryptology 2017, Issue 4:

- Submission: 1 September 2017
- Rebuttal: 8-11 October 2017
- Decision: 1 November 2017
- Camera-ready deadline for accepted papers (and conditionally accepted): 28 November 2017

Volume IACR Transactions on Symmetric Cryptology 2018, Issue 1:

- Submission: 23 November 2017
- Rebuttal: 4-8 January 2018
- Decision: 23 January 2018
- Camera-ready deadline for accepted papers (and conditionally accepted): 23 February 2018

General Chair

Elena Andreeva, KU Leuven, Belgium

Program Chairs/Co-Editors-in-Chief

Florian Mendel, Infineon Technologies AG, Germany
María Naya-Plasencia, Inria, France

Program Committee/Editorial Board

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 and editorial boards to detect parallel submissions and the IACR policy 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. Submissions should be typeset in the LaTeX style available at `http://tosc.iacr.org/index.php/ToSC/pages/view/Template`. The page limit is 20 pages excluding bibliography. Authors are encouraged to include supplementary material at the end of the paper, such as test values or source code that can assist reviewers in verifying the validity of the results; this material will not be included in the page count.

If authors believe that more details are essential to substantiate the claims of their paper or to provide proofs, they can submit a longer paper up to 40 pages (instead of up to 20); this should be indicated by ending the title with "(Long Paper)". For long papers, the decision may be deferred to the next round at the discretion of the editors-in-chief (and to the next FSE for issue 1).

Submissions not meeting these guidelines risk rejection without consideration of their merits. The IACR Transactions on Symmetric Cryptology journal only accepts electronic submissions in PDF format. A detailed description of the electronic submission procedure will be available at http://tosc.iacr.org/index.php/ToSC/pages/view/Submission. **The authors of submitted papers guarantee that their paper will be presented at the FSE 2018 conference if it is accepted**.

In order to improve the quality of the review process, authors will be given the opportunity to enter a **rebuttal** between the indicated dates, after receiving the reviews.

Conference Information and Stipends

The primary source of information is the conference website. A limited number of stipends are available to those unable to obtain funding to attend the conference. Students, whose papers are accepted and who will present the paper themselves, will receive a registration fee waiver funded by the IACR Cryptography Research fund for students; they are encouraged to apply for additional assistance if needed. Requests for stipends should be sent to the general chair.

Contact Information

All correspondence and/or questions should be directed to either of the organizational committee members:

General Chair
Elena Andreeva, KU Leuven, Belgium
fse2018@esat.kuleuven.be

Program Chairs/Co-Editors-in-Chief
Florian Mendel, Infineon Technologies AG, Germany
María Naya-Plasencia, Inria, France
tosc_editors18@iacr.org