



# Fast Software Encryption 2019

## IACR Transactions on Symmetric Cryptology

### Call for Papers

#### *General Information on FSE 2019*

---

#### **26th International Conference Fast Software Encryption (FSE 2019)**

Paris, France

March 25-28

General information: <https://fse.iacr.org/2019/>

Submission server: <http://tosc.iacr.org/index.php/ToSC/pages/view/Submission>

FSE 2019 is the 26th edition of Fast Software Encryption conference, and one of the area conferences organized by the International Association for Cryptologic Research (IACR). FSE 2019 will take place in Paris, on March 25-28, 2019. Original research papers on symmetric cryptology are invited for submission to FSE 2019. 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 2017, FSE 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 2017, 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 2019, 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 2019 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 2019 / IACR Transactions on Symmetric Cryptology 2018/2019***

---

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

#### **IACR Transactions on Symmetric Cryptology, Volume 2018, Issue 2:**

- Submission: 1 March 2018
- Rebuttal: 4-7 April 2018
- Decision: 1 May 2018
- Camera-ready deadline for accepted papers (and conditionally accepted): 28 May 2018

#### **IACR Transactions on Symmetric Cryptology, Volume 2018, Issue 3:**

- Submission: 1 June 2018
- Rebuttal: 4-7 July 2018
- Decision: 1 August 2018
- Camera-ready deadline for accepted papers (and conditionally accepted): 28 August 2018

#### **IACR Transactions on Symmetric Cryptology, Volume 2018, Issue 4:**

- Submission: 1 September 2018
- Rebuttal: 4-7 October 2018
- Decision: 1 November 2018
- Camera-ready deadline for accepted papers (and conditionally accepted): 28 November 2018

#### **IACR Transactions on Symmetric Cryptology, Volume 2019, Issue 1:**

- Submission: 23 November 2018
- Rebuttal: 2-6 January 2019
- Decision: 23 January 2019
- Camera-ready deadline for accepted papers (and conditionally accepted): 23 February 2019

### ***General Chair***

---

Jérémy Jean, ANSSI, Paris

### ***Program Chairs/Co-Editors-in-Chief***

---

Florian Mendel, Infineon Technologies, Germany

Yu Sasaki, NTT Secure Platform Laboratories, Japan

### ***Program Committee/Editorial Board***

---

Frederik Armknecht, University of Mannheim, Germany

Subhadeep Banik, EPFL, Switzerland

Daniel J. Bernstein, University of Illinois at Chicago, USA

Alex Biryukov, University of Luxembourg, Luxembourg

Christina Boura, University of Versailles, France

Anne Canteaut, Inria, France

Carlos Cid, Royal Holloway University of London, United Kingdom

Joan Daemen, Radboud University, Netherlands and STMicroelectronics, Belgium  
Patrick Derbez, University of Rennes 1, France  
Itai Dinur, Ben Gurion University, Israel  
Christoph Dobraunig, TU Graz, Austria  
Orr Dunkelman, University of Haifa, Israel  
Maria Eichlseder, TU Graz, Austria  
Jian Guo, NTU, Singapore  
Takanori Isobe, University of Hyogo, Japan  
Tetsu Iwata, Nagoya University, Japan  
Jérémy Jean, ANSSI, France  
Pierre Karpman, Université Grenoble Alpes, France  
Nathan Keller, Bar-Ilan University, Israel  
Stefan Kölbl, DTU, Denmark  
Virginie Lallemand, University of Bochum, Germany  
Gregor Leander, University of Bochum, Germany  
Jooyoung Lee, KAIST, Korea  
Gaëtan Leurent, Inria, France  
Stefan Lucks, Bauhaus-Universität Weimar, Germany  
Subhamoy Maitra, ISI, India  
Willi Meier, FHNW, Switzerland  
Bart Mennink, Radboud University, Netherlands  
Nicky Mouha, NIST, USA  
Maria Naya-Plasencia, Inria, France  
Samuel Neves, University of Coimbra, Portugal  
Ivica Nikolic, National University of Singapore, Singapore  
Kaisa Nyberg, Aalto University, Finland  
Bart Preneel, KU Leuven, Belgium  
Arnab Roy, University of Bristol, United Kingdom  
Martin Schläffer, Infineon Technologies, Germany  
Yannick Seurin, ANSSI, France  
Hadi Soleimany, Shahid Beheshti University, Iran  
Ling Song, NTU, Singapore and Chinese Academy of Sciences, China  
Marc Stevens, CWI, Netherlands  
Elmar Tischhauser, DTU, Denmark  
Yosuke Todo, NTT Secure Platform Laboratories, Japan  
Gilles Van Assche, STMicroelectronics, Belgium  
Damian Vizár, EPFL, Switzerland  
Lei Wang, Shanghai Jiao Tong University, China

### ***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 <https://github.com/Cryptosaurus/iacrtrans/archive/master.zip>. 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 the submission. 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).

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 2019 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.

### ***Conflicts of Interest***

---

Authors, program committee members, and reviewers must follow the new IACR Policy on Conflicts of Interest available at <http://tosc.iacr.org/Call#coi>.

### ***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***

Jérémy Jean, ANSSI Paris  
fse2019@iacr.org

#### ***Program Chairs/Co-Editors-in-Chief***

Florian Mendel, Infineon Technologies, Germany  
Yu Sasaki, NTT Secure Platform Laboratories, Japan  
tosc\_editors19@iacr.org