



# Fast Software Encryption 2022

## IACR Transactions on Symmetric Cryptology

### Call for Papers

#### *General Information on FSE 2022*

---

#### **The 28th International Conference on Fast Software Encryption (FSE 2022)**

Athens, Greece

March 20-25

General information: <https://fse.iacr.org/2022/>

Submission information: <https://tosc.iacr.org/Submission>

FSE 2022 is the 28th edition of Fast Software Encryption conference, and one of the area conferences organized by the International Association for Cryptologic Research (IACR). FSE 2022 will take place in Athens on March 20-25, 2022. Original research papers on symmetric cryptology are invited for submission to FSE 2022. The scope of FSE concentrates on fast and secure primitives and modes 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.

Starting 2020, ToSC also accepts submissions for **addendum** and **errata** papers. Addendum papers aim at extending an existing ToSC paper in a novel, yet succinct way. The title of such papers must begin with "Addendum to", followed by the title of the initial paper. Errata papers aim at correcting an error in an existing ToSC paper. Their title must begin with "Errata to", followed by the title of the corrected paper. Addendum and errata papers are limited to 4 pages excluding bibliography and will not be presented at FSE.

#### *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 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: <https://tosc.iacr.org/FAQ>.

Due to the cancellation of FSE 2021 as a consequence of the COVID-19 pandemic, papers from the following six issues of ToSC will be presented at FSE 2022: 2020(4), 2021(1), 2021(2), 2021(3), 2021(4) and 2022(1).

This call for papers refers to the last four issues. 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, “**major revision**” decisions, in which case authors are provided with a list of requested changes that are likely to result in the paper being accepted, or “**reject and resubmit**” decisions when the reviewers see some potential in the paper, but there are significant issues to address before the paper can be properly evaluated.

In case of “major revision” decision, authors are invited to revise and resubmit their article to one of the following two submission deadlines (respectively one month and four months after the notification), together with a statement explaining how the reviews have been addressed. We endeavor to assign the same reviewers to revised versions. Major revision papers will be considered to be under review during the four months window after the notification; authors must formally withdraw their paper if they wish to submit it to another journal or a conference/workshop with proceedings. If the paper is resubmitted after more than four months, it will be treated as a new submission.

In case of a “reject and resubmit” decision, the authors can resubmit their article, but must wait at least for the second next submission deadline (four months after the notification), because the paper requires significant editorial or technical changes. These papers are not considered under review, and the revision may receive the same reviewers or different reviewers. Rejected papers can only be resubmitted after significantly improving the results. Authors of rejected papers must wait at least for the third submission deadline (seven months after the notification) before resubmitting.

Papers accepted for publication before the end of January 2022 will be presented at that year’s conference. Note that papers submitted in November can be deferred to the next year’s conference in case of “major revision”. Moreover it is **mandatory that accepted papers at the IACR Transactions on Symmetric Cryptology journal are presented at the corresponding FSE event.**

### ***Timeline for FSE 2022 / IACR Transactions on Symmetric Cryptology 2021/2022***

---

All upcoming deadlines are 12:00:00 (**noon**) Greenwich Mean Time (UTC)

#### **IACR Transactions on Symmetric Cryptology, Volume 2021, Issue 2:**

- Submission: 1 March 2021
- Rebuttal: 6-9 April 2021
- Decision: 1 May 2021
- Camera-ready deadline for accepted papers (and conditionally accepted): 28 May 2021

#### **IACR Transactions on Symmetric Cryptology, Volume 2021, Issue 3:**

- Submission: 1 June 2021
- Rebuttal: 6-9 July 2021
- Decision: 1 August 2021
- Camera-ready deadline for accepted papers (and conditionally accepted): 28 August 2021

#### **IACR Transactions on Symmetric Cryptology, Volume 2021, Issue 4:**

- Submission: 1 September 2021
- Rebuttal: 5-8 October 2021
- Decision: 1 November 2021
- Camera-ready deadline for accepted papers (and conditionally accepted): 28 November 2021

#### **IACR Transactions on Symmetric Cryptology, Volume 2022, Issue 1:**

- Submission: 23 November 2021
- Rebuttal: 3-6 January 2022
- Decision: 23 January 2022
- Camera-ready deadline for accepted papers (and conditionally accepted): 23 February 2022

### ***General Chair***

---

Christina Boura, University of Versailles, France

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

---

Itai Dinur, Ben-Gurion University, Israel

Bart Mennink, Radboud University, The Netherlands

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

---

Elena Andreeva, Technical University of Vienna, Austria

Tomer Ashur, TU Eindhoven, The Netherlands and KU Leuven, Belgium

Subhadeep Banik, EPFL, Switzerland

Zhenzhen Bao, NTU, Singapore

Christof Beierle, Ruhr University Bochum, Germany

Xavier Bonnetain, University of Waterloo, Canada

Christina Boura, University of Versailles, France

Patrick Derbez, Université Rennes, CNRS and IRISA, France

Christoph Dobraunig, Lamarr Security Research, Austria

Sébastien Duval, University of Versailles, France

Maria Eichlseder, Graz University of Technology, Austria

Lorenzo Grassi, Radboud University, The Netherlands

Vincent Grosso, Jean Monnet University, CNRS, France

Jian Guo, NTU, Singapore

Andreas Hülsing, TU Eindhoven, The Netherlands

Takanori Isobe, University of Hyogo and NICT, Japan

Tetsu Iwata, Nagoya University, Japan

Jérémy Jean, ANSSI, France

Pierre Karpman, Université Grenoble Alpes, France

Nathan Keller, Bar-Ilan University, Israel

Stefan Kölbl, Google, Switzerland

Virginie Lallemand, CNRS, France

Jooyoung Lee, KAIST, Korea

Stefan Lucks, Bauhaus-Universität Weimar, Germany

Willi Meier, FHNW, Switzerland

Florian Mendel, Infineon Technologies, Germany

Brice Minaud, Inria and ENS, France

Kazuhiko Minematsu, NEC, Japan

Nicky Mouha, NIST, United States

Kaisa Nyberg, Aalto University, Finland

Léo Perrin, Inria, France

Thomas Peyrin, NTU, Singapore

Yann Rotella, University of Versailles, Université Paris-Saclay, France

Yu Sasaki, NTT Secure Platform Laboratories, Japan

Yannick Seurin, ANSSI, France

Siang Meng Sim, DSO, Singapore

Hadi Soleimany, Shahid Beheshti University, Iran

Ling Song, Jinan University, China

Siwei Sun, Chinese Academy of Sciences, China

Yosuke Todo, NTT Secure Platform Laboratories, Japan

Aleksei Udovenko, CryptoExperts, France

Damian Vizár, CSEM, Switzerland

Qingju Wang, University of Luxembourg, Luxembourg  
Friedrich Wiemer, cryptosolutions and Robert Bosch, Germany

### ***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 `iacrtrans` L<sup>A</sup>T<sub>E</sub>X class, available at <https://github.com/Cryptosaurus/iacrtrans/releases>. The class documentation includes examples and instructions to easily convert a paper written with the `l1ncs` class.

The page limit for regular papers is 20 pages excluding bibliography. Authors are encouraged to include supplementary material that can assist reviewers in verifying the validity of the results at the end of the paper. Supplementary material that does not require extra reviewing effort (such as test values, source code, or charts) will be published with the paper, but are not included in the page count. However, material that requires careful reviewing (such as proofs of the main theorems) will be included in the page count, even if they are written as appendices.

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 (with no page limit); this should be indicated by ending the title with "(Long Paper)" for the submission. For long papers of up to 40 pages, the decision may be deferred to the next round at the discretion of the editors-in-chief (and to the next FSE if submitted in November). For papers longer than 40 pages, the first round of review may be dedicated only to evaluating whether the length of the papers is justified by the scientific contribution. Moreover, the decision may be deferred by one or more rounds at the discretion of the editors-in-chief.

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 is available at <https://tosc.iacr.org/Submission>. **The authors of submitted papers guarantee that their paper will be presented at the FSE 2022 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 <https://tosc.iacr.org/Call#coi>. In particular, we require authors to list potential conflict of interest with editorial board members at the time of submission, taking into account the set of all authors, and to explain the reason of each conflict.

### ***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***

Christina Boura, University of Versailles, France

[fse2022@iacr.org](mailto:fse2022@iacr.org)

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

Itai Dinur, Ben-Gurion University, Israel

Bart Mennink, Radboud University, The Netherlands

[tosc\\_editors22@iacr.org](mailto:tosc_editors22@iacr.org)