# IACR Transactions on Symmetric Cryptology

Special Issue on

# Designs for the NIST Lightweight Standardisation Process

## Call for Papers

### *Special Issue on the NIST Lightweight Standardisation Process*

The National Institute of Standards and Technology (NIST) is currently running a standardisation process for new lightweight cryptography algorithms. This process started with a call for algorithms that received 57 submissions in February 2019, and 32 of them advanced to the second round in August 2019.
This special issue of the *IACR Transactions on Symmetric Cryptology* will be devoted to algorithms designed for this standardisation effort, and selected in the second round of the competition.

Information that differs from the usual ToSC Call for Papers will be given in blue.

### *Timeline*

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

- Submission: 10 December 2019
- Rebuttal: 25-28 January 2020
- Decision: 15 February 2020 (for papers of at most 20 pages)
- Camera-ready deadline for accepted papers (and conditionally accepted): 15 March 2020

### *Publication Information*

Submissions will be reviewed with the same scientific requirements as regular ToSC submissions in terms of security and novelty. For reviewing submissions to this special issue, we will generally consider a scheme that has been selected by NIST for the second round to be worthy of interest.

Authors are requested to structure their papers as standard design submissions to ToSC which emphasize the novel aspects of their schemes (such as security proofs or analysis, or design rationale). Submissions should include at least a clear and self-contained specification, rationale for the design, security analysis and implementation results.
If parts of the designs have been published previously, or are in the process of being published, the submission should contain a minimum of 30% *new scientific contributions* (such as improved security proofs or analysis, interesting implementation results, or rationale for unpublished parts of the design).

Papers must be submitted on a dedicated server, available at:
https://secure.iacr.org/websubrev/tosc20_nist/submit/

Accepted papers will be published in the special issue of ToSC, and authors will be invited to give a short presentation at FSE. For more information about FSE, see the official website: https://fse.iacr.org/.

Submissions to the special issue will not count against the submission limits for editorial board members.

### *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 should **not** be anonymous. It should begin with a title, author names and affiliations, a short abstract, and a list of keywords. Submissions should be typeset in the `iacrtrans` LaTeX class, available at https://github.com/Cryptosaurus/iacrtrans/releases. The class documentation includes examples and instructions to easily convert a paper written with the `llncs` class.

We will not enforce a page limit for this special issue, but authors are strongly encouraged to fit their contributions into 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. For papers with more than 20 pages of content, the decision may be deferred to a later date 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. 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.

If some papers require major revisions, they will have to be resubmitted with a timeline that will be determined later.

### *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.

### *Contact Information*

All correspondence and/or questions should be directed to the co-editors-in-chief:

***Co-Editors-in-Chief***
Itai Dinur, Ben-Gurion University, Israel
Gaëtan Leurent, Inria, France
tosc_editors21@iacr.org

### *Co-Editors-in-Chief*

Itai Dinur, Ben-Gurion University, Israel
Gaëtan Leurent, Inria, France