Journal of Cryptology
Special Issue on CAESAR
Call for Papers

CAESAR (Competition for Authenticated Encryption: Security, Applicability, and Robustness)[1] is a competition to identify a portfolio of authenticated ciphers that (1) offer advantages over AES-GCM and (2) are suitable for widespread adoption. The competition was announced in 2013, and was completed in February 2019 with the announcement of the final portfolio.

This special issue of the Journal of Cryptology will be devoted to advances in cryptology related to the development of CAESAR. Papers are solicited on topics including, but not limited to:

- security and/or implementation analysis of the CAESAR final portfolio;
- comparison or tools for comparison of security and/or implementation of the CAESAR final portfolio with related authenticated ciphers.

Submissions should be related to the CAESAR final portfolio. Authors of papers analyzing the security and/or implementation of related authenticated ciphers are encouraged to emphasize the relation of their work to the CAESAR final portfolio.

Dates

Submission Deadline:	December 2, 2019
Publication date (tentative):	December 1, 2020

Instructions for Authors

Original paper submissions should be made following the standard instructions for the Journal of Cryptology (`http://www.iacr.org/jofc/`) and submitted via the Journal of Cryptology submission site (`https://www.editorialmanager.com/jcryptology/`). On the submission site, there is a field to enter comments to the publication office, where authors can note that they wish their paper to be considered for this special issue. Submissions will be refereed by the usual standards of the Journal of Cryptology.

Guest Editor

Enquiries may be directed to the guest editor: Tetsu Iwata, Nagoya University: `tetsu.iwata@nagoya-u.jp`.

[1] `https://competitions.cr.yp.to/index.html`