Journal of Cryptology
Special Issue on TLS 1.3
Call for Papers

The Transport Layer Security (TLS) protocol is the most important cryptographic protocol on the Internet. After several years of intensive attack on earlier versions of TLS up to version 1.2, the IETF has developed a new standard for TLS 1.3 with the primary goals of improving security, removing old cryptographic algorithms, and decreasing latency. The TLS 1.3 specification became IETF Proposed Standard RFC 8446 in August 2018.

This special issue of the Journal of Cryptology will be devoted to advances in cryptology related to the TLS 1.3 development process. Papers are solicited on topics including, but not limited to:

- security analysis of TLS 1.3 using various formal techniques, possibly focussing on specific protocol subsets;
- analysis of security and efficiency tradeoffs within TLS 1.3;
- technical comparison of TLS 1.3 with related protocols;
- lessons learned from the TLS 1.3 development process.

Papers should relate to the final standardized version of TLS 1.3. Authors of papers attacking and/or repairing earlier draft versions of TLS 1.3 are encouraged to revisit the final version of TLS 1.3, and update the analysis or tools to ensure that any attacks are not possible and/or that fixes remain effective.

Dates

Submission Deadline:	31 October 2019
Preliminary Decisions:	30 April 2020
Publication date (tentative):	31 August 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 at 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: Colin Boyd, Norwegian University of Science and Technology (NTNU): `colin.boyd@ntnu.no`.