IACR Transactions on Symmetric Cryptology
ISSN 2519-173X, Vol. 2020, No. 1, pp. 1–5. DOI:10.13154/tosc.v2020.i1.1-5

Preface to Volume 2020, Issue 1

Gaëtan Leurent[1] and Yu Sasaki[2]

[1] Inria, Paris, France
[2] NTT Secure Platform Laboratories, Tokyo, Japan

IACR Transactions on Symmetric Cryptology (ToSC) is a forum for original results in all areas of 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.

ToSC implements an open-access journal/conference hybrid model following some other communities in computer science. All articles undergo a journal-style reviewing process and accepted papers are published in gold open access (in our case the Creative Commons License CC-BY 4.0). The review procedures that we have followed strictly adhere to the traditions of the journal world. Full papers are assigned to the members of the Editorial Board. These members write detailed and careful reviews (usually without relying on subreviewers). Moreover, we have had a rebuttal phase, allowing authors to respond to the review comments before the final decisions. If necessary, the review process enables further interactions between the authors and the reviewers, mediated by the Co-Editors-in-Chief. Detailed discussions among the reviewers lead to one of the following four decisions for each paper: ACCEPT, in which case the authors submit their final camera-ready manuscript after editorial corrections; ACCEPT with MINOR REVISION, which means that the authors revise their manuscript and go through one or more iterations and reviews of the manuscript until the comments have been addressed in a satisfactory way; MAJOR REVISION, which means that the authors are requested to make major changes to their manuscript before submitting again in one of the next rounds; and REJECT, which means that the manuscript is deemed to be not suitable for publication in ToSC.

The review process shares with the high quality conferences that it is double-blind and adheres to a strict timing; but unlike a traditional conference, there are multiple submission deadlines per year. Most papers are notified of the decision two months after submission, but the decision can be deferred for long papers. This year, we received a few very long papers, and we decided to experiment with a new procedure where we first ask reviewers to judge whether the length is justified by the scientific contribution, and we only proceeded with the scientific review in a second phase. Each paper received at least three reviews; for submissions by Editorial Board members this was increased to at least four.

Overall, we are very pleased with the quality and quantity of submissions, the detailed review reports written by the reviewers and the substantial efforts by the authors to further improve the quality of their work. We think that the review process, and in particular the use of major revisions, leads to an increased quality of the papers that are published.

The papers selected by the Editorial Board for publication are presented at the conference Fast Software Encryption (FSE). This gives the authors the opportunity to advertise their results and engage in discussions on further work. In 2020, FSE was originally scheduled for March 22-26, 2020 in Athens, Greece. However, the worldwide outbreak of COVID-19 led to travel restrictions and social distancing measures in many countries. In early March, the Greek Health Ministry decided to suspend all conference

Published: 2020-05-07

events in Greece. Therefore, FSE was postponed to November 8-12, 2020 in the same place, and we expect that papers published in ToSC Volume 2019, Issues 2-4 and Volume 2020, Issue 1 will be presented there. For Volume 2019, Issue 2, we received 25 submissions, out of which 8 were accepted, 5 of these after minor revisions; 3 papers received a major revision decision and the decision was deferred to the next issue for 1 paper. For Volume 2019, Issue 3, we received 30 submissions, out of which 9 were accepted, 6 of these after minor revisions; 11 papers received a major revision decision. For Volume 2019, Issue 4, we received 49 submissions, out of which 17 were accepted, 8 of these after minor revisions; 7 papers that received a major revision decision, 1 paper was accepted in the Special Issue on Designs for the NIST Lightweight Standardisation Process as a minor revision, and the decision was deferred to the next issue for 2 papers. For Volume 2020, Issue 1, we received 41 submissions, out of which 14 were accepted, 9 of these after minor revisions; the number of papers that received a major revision decision was 6 and the decision was deferred to the next issue for 2 papers, 1 of them as a minor revision.

Besides the 48 selected talks, the program will include two invited talks by Kazuhiko Minematsu on security of OCB2 and Thomas Peyrin on tweakable block ciphers. As it is tradition for FSE, the Editorial Board also selected a best paper, based on the scientific quality and contribution. The Editorial Board has decided to give the award to the paper by Yaobin Shen and Lei Wang entitled "On Beyond-Birthday-Bound Security: Revisiting the Development of ISO/IEC 9797-1 MACs".

We would like to thank the authors of all submissions for contributing high quality submissions and giving us the opportunity to compile a good and diverse program. In particular, we would like to thank the Editorial Board members; we value their hard work and dedication to write constructive and detailed reviews and to engage in interesting discussions. Many Editorial Board members spent additional time as shepherds to help the authors improving their works. We would also like to thank the subreviewers for their efforts. We are profoundly indebted to the conference General Chair Christina Boura for her hard work to prepare the conference and handle the unprecedented interruption by the COVID-19 pandemic. We also would like to thank Anne Canteaut, Shai Halevi, Gregor Leander, Friedrich Wiemer, and Phil Hebborn for their work and support. Finally, we would like to thank Inpher and Rambus for their generous support of the conference.

We hope that the papers in this volume of IACR Transactions on Symmetric Cryptology (ToSC) prove valuable and we are glad to see that ToSC is becoming the leading international venue publishing the top research on symmetric cryptology.

March 2020

Gaëtan Leurent
Yu Sasaki

Editorial Board

External reviewers

Benoit Cogliati
Vasily Mikhalev
Shahram Rasoolzadeh
Qingju Wang