IACR Transactions on Symmetric Cryptology
ISSN 2519-173X, Vol. 2021, No. 1, pp. 1–4. DOI:10.46586/tosc.v2021.i1.1-4

Preface to Volume 2021, Issue 1

Itai Dinur[1] and Gaëtan Leurent[2]

[1] Ben-Gurion University, Beer Sheva, Israel
[2] Inria, Paris, France

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.

The ToSC review process strives to maintain a high quality of published articles. Full papers are assigned to at least three members of the Editorial Board; for submissions by Editorial Board members this was increased to at least four. 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. The Editorial Board can also decide to ask for a minor or major revision of the paper when changes are deemed necessary to improve its quality. Furthermore, starting 2020, a "reject and resubmit" decision can be given in case the Editorial Board sees some potential in a paper, but there are significant issues to address before it can be properly evaluated.

Starting 2020, ToSC also accepts submissions of addendum and errata papers. Addendum papers aim at extending an existing ToSC paper in a novel, yet succinct way. Errata papers aim at correcting an error in an existing ToSC paper.

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. The worldwide outbreak of COVID-19 has led to changes in the FSE schedule. FSE 2020 was held virtually in November 9-13, with paper from issues: 2019(2), 2019(3), 2019(4), 2020(1), 2020(2), 2020(3) and 2020(S1). FSE 2021 was canceled, while FSE 2022 will be held in Athens, Greece on March 20-25, with papers from the following issues of ToSC: 2020(4), 2021(1), 2021(2), 2021(3), 2021(4) and 2022(1). In addition to the scientific papers from the journal, FSE 2020 had two invited talks, by Kazuhiko Minematsu on security of OCB2 and Thomas Peyrin on tweakable block ciphers, and two *Ask Me Anything* sessions with Joan Daemen and Kaisa Nyberg.

Table 1 gives the submission statistics for issues 2020(2), 2020(3), 2020(4) and 2021(1). For example, for Volume 2020, Issue 3, we received 30 regular submissions, out of which

Table 1: Submission statistics for issues 2020(2), 2020(3), 2020(4), 2021(1)

Volume (Issue)	Regular Submissions	Accepted (Minor Revision)	Major Revision	Decision Deferred	Reject and Resubmit	Errata
2020(2)	29	5(4)	4	0	8	0
2020(3)	30	10(4)	5	0	3	1
2020(4)	47	9(3)	7	1	4	0
2021(1)	37	13(5)	5	0	8	0

10 were accepted (including 4 minor revisions) and 5 papers received a major revision decision. The decision for none of the submissions was deferred to the next cycle. Out of the remaining rejected papers, 3 received a "reject and resubmit" decision. We further accepted one errata paper.

As it is tradition for FSE, the Editorial Board also selected best papers, based on the scientific quality and contribution. This year the Editorial Board has decided to give the award to two papers: "Catching the Fastest Boomerangs – Application to SKINNY" by Stéphanie Delaune, Patrick Derbez and Mathieu Vavrille, and "Cryptanalysis of LowMC instances using single plaintext/ciphertext pair" by Subhadeep Banik, Khashayar Barooti, F. Betül Durak and Serge Vaudenay.

We would like to thank the authors of all submissions for contributing high quality submissions. 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 are deeply grateful of the work of Kevin McCurley and Kay McKelly who organized the virtual conference FSE 2020, and Christina Boura who had planned FSE 2020 in Athens, and will be the general chair of FSE 2022. We also would like to thank Anne Canteaut, Gregor Leander, Friedrich Wiemer, Phil Hebborn, and Linda Groß for their work and support. 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 2021

Itai Dinur
Gaëtan Leurent

Editorial Board

External reviewers