IACR Transactions on Symmetric Cryptology
ISSN 2519-173X, Vol. 2023, No. 1, pp. 1–4. DOI:10.46586/tosc.v2023.i1.1-4

Preface to Volume 2023, Issue 1

Christina Boura[1] and Bart Mennink[2]

[1] University of Versailles, Versailles, France
[2] Radboud University, Nijmegen, The Netherlands

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, the Editorial Board can give a "reject and resubmit" decision in case a submission is considered to have potential, but there are significant issues to address before it can be properly evaluated.

Next to regular submissions, ToSC also accepts submissions of addendum and corrigendum papers. Addendum papers aim at extending an existing ToSC paper in a novel, yet succinct way. Corrigendum 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 advertize their results and engage in discussions on further work. In 2023, FSE was held during March 20-24, 2023. For the first time, and for reasons related to the COVID-19 pandemic, there were two parallel and perfectly synchronized events. The main one in Beijing, China, and a mirror one in Kobe, Japan. Speakers and other participants not being able to attend either location participated remotely. During the conference, papers from the following four issues of ToSC have been presented at FSE 2023: 2022(2), 2022(3), 2022(4) and 2023(1). In addition to the scientific papers from the journal, FSE 2023 had two invited talks: Siwei Sun on the cryptanalysis of ARX ciphers and Yosuke Todo on the story behind the development of the division property.

Table 1 gives the submission statistics for issues 2022(2), 2022(3), 2022(4), and 2023(1). For example, for Volume 2022, Issue 4, we received 53 regular submissions, out of which 11

Table 1: Submission statistics for issues 2022(2), 2022(3), 2022(4), and 2023(1)

Volume (Issue)	Regular Submissions	Accepted (Minor Revision)	Major Revision	Reject and Resubmit	Deferred	SoK Submitted (Accepted)
2022(2)	38	13(6)	6	4	0	0/0
2022(3)	44	14(9)	5	3	0	1/0
2022(4)	53	11(4)	2	13	3	0/0
2023(1)	41	10(1)	6	7	0	1/1

were accepted (including 4 minor revisions) and 2 papers received a major revision decision. Out of the remaining rejected papers, 13 received a "reject and resubmit" decision. Issue 2022(4) received a record high number of submissions, including many long papers, and in order to keep the editorial quality high, we decided to defer two submissions to the next round. The publication of one accepted submission of 2022(4) was deferred to the next round at the authors' request. In total, we received 2 SoK submissions (one in 2022(3) and one in 2023(1)), one of which got accepted. None of the submitted papers to any of the four issues was an addendum or corrigendum 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 the papers "Mind Your Path: on (Key) Dependencies in 2 Differential Characteristics" by Thomas Peyrin and Quan Quan Tan, and "Hybrid Code Lifting on Space-Hard Block Ciphers — Application to Yoroi and SPNbox" by Yosuke Todo and Takanori Isobe.

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 thankful to Bin Zhang and Meiqin Wang for the organization of FSE 2023 in Beijing, China, and to Takanori Isobe and Fukang Liu for the organization of the mirror event in Kobe, Japan. We would also like to thank Kevin McCurley and Kay McKelly for making it possible to hold FSE 2023 as a hybrid event. We are moreover thankful to Kevin for his help with the review process management system. We also would like to thank Anne Canteaut, Gregor Leander, Christof Beierle 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 2023

Christina Boura
Bart Mennink

Editorial Board