IACR Transactions on Symmetric Cryptology
ISSN 2519-173X, Vol. 2025, No. 1, pp. 1–4. DOI:10.46586/tosc.v2025.i1.1-4

Preface to Volume 2025, Issue 1

Christoph Dobraunig[1] and Kazuhiko Minematsu[2,3]

[1] Intel Labs, Hillsboro, USA
[2] NEC, Kawasaki, Japan
[3] Yokohama National University, Yokohama, 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 *diamond* open access (in our case the Creative Commons License CC-BY 4.0). The review procedures 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 pleased with the quality and quantity of submissions, the reviewers' detailed review reports and the substantial efforts by the authors to 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 authors the opportunity to advertise their results and engage in discussions on further work. For FSE 2025, we launched the artifact evaluation for the accepted papers. Patrick Derbez (University of Rennes, France) served as the chair of the artifact evaluation committee (AEC). Each artifact submission was reviewed by two reviewers from the AEC. The review process was single-blinded (submitters are not anonymous) and interactive between the submitters and the reviewers via the submission system if needed. For each ToSC issue we set a submission deadline for artifact evaluation.

In 2025, FSE was held in Rome, Italy during March 17 to 21, 2025. Papers from the following four issues of ToSC have been presented at FSE 2025: 2024(2), 2024(3), 2024(4) and 2025(1). In addition to the scientific papers from the journal, FSE 2025 had

Table 1: Submission statistics for issues 2024(2), 2024(3), 2024(4), and 2025(1). A cell $x(y)$ in "SoK" column denotes y accepted submissions among x SoK submissions. Same for "Cor." for corrigendum and "Add." for addendum.

Volume (Issue)	Submissions	Accepted (Minor Revision)	Major Revision	Reject and Resubmit	Deferred	SoK (Acc)	Cor. (Acc)	Add. (Acc)
2024 (2)	35	13 (9)	5	5	0	0 (0)	0 (0)	0 (0)
2024 (3)	28	8 (4)	3	5	0	1 (0)	0 (0)	1 (1)
2024 (4)	44	7 (3)	9	17	0	1 (0)	0 (0)	0 (0)
2025 (1)	60	19 (8)	6	12	1	2 (1)	1 (1)	0 (0)

two invited talks from Anne Canteaut and Tetsu Iwata. Anne's talk, entitled as "Stream Ciphers Strike Back", was about the recent applications of stream ciphers in the new contexts. Tetsu's talk entitled as "Two Decades of CMAC", was about CMAC, a NIST recommended block cipher mode for authentication, and he revisited research results on CMAC.

Table 1 gives the submission statistics for issues 2024(2), 2024(3), 2024(4) and 2025(1). For example, for Volume 2025, Issue 1, we received 60 submissions. Among them, 19 were accepted (including 8 minor revisions) and 6 papers received a major revision decision. One paper got deferment as we need more resources for quality reviewing. Out of the remaining rejected papers, 12 received a "reject and resubmit" decision. Regarding SoK/Corrigendum/Addendum, we received one SoK submission in 2024 (3), one in 2024 (4), and two in 2025 (1), and one got accepted after a minor revision. One corrigendum was submitted in 2025 (1) and one addendum was submitted in 2024 (3). Both got accepted. At the time of writing, four artifact submissions got accepted.

As it is tradition for FSE, the Editorial Board also selected best papers, based on scientific quality and contribution. This year, the Editorial Board has decided to give the award to the paper "Permutation-Based Hash Chains with Application to Password Hashing" by Charlotte Lefevre and Bart Mennink.

We would like to thank the authors of all submissions for contributing high quality papers. Furthermore, we would like to thank the Editorial Board members; we value their hard work and dedication in writing constructive and detailed reviews and engaging in interesting discussions. Many Editorial Board members spent additional time as shepherds to help the authors to improve their works. We also would like to thank Patrick Derbez and the members of AEC for conducting artifact evaluation, which was surely challenging as this is the first time for ToSC.

We are thankful to Lorenzo Grassi and Marco Pedicini for the organization of FSE 2025 in Rome, Italy. We are moreover thankful to Kevin McCurley for his great help with the review process management system. We also would like to thank Orr Dunkelman, 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 2025

Christoph Dobraunig
Kazuhiko Minematsu

Editorial Board