IACR Transactions on Symmetric Cryptology
ISSN 2519-173X, Vol. 2024, No. 1, pp. 1–4. DOI:10.46586/tosc.v2024.i1.1-4

Preface to Volume 2024, Issue 1

Christina Boura[1] and Kazuhiko Minematsu[2,3]

[1] University of Versailles, Versailles, France
[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 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 2024, FSE was held during March 25 to 29, 2024 in Leuven, Belgium. During the conference, papers from the following four issues of ToSC have been presented at FSE 2024: 2023(2), 2023(3), 2023(4) and 2024(1). It has to be noted that for the first time, presentation of accepted papers to ToSC was not mandatory but presentations could only be given in person. Despite this new rule, we were very happy to attest that all accepted papers were at the end presented. In addition to the scientific papers from the journal, FSE 2024 had two invited talks: Maria Eichlseder on tools for cryptanalysis and Gaëtan Leurent on cryptanalysis beyond primitives.

Table 1: Submission statistics for issues 2023(2), 2023(3), 2023(4), and 2024(1)

Volume (Issue)	Regular Submissions	Accepted (Minor Revision)	Major Revision	Reject and Resubmit	Deferred	SoK Submitted (Accepted)
2023 (2)	35	8 (5)	4	6	0	1 (1)
2023 (3)	38	7 (4)	8	8	0	0 (0)
2023 (4)	57	18 (6)	9	8	0	0 (0)
2024 (1)	45	15 (9)	4	7	0	0 (0)

Table 1 gives the submission statistics for issues 2023(2), 2023(3), 2023(4), and 2024(1). For example, for Volume 2023, Issue 4, we received 57 regular submissions, which is a record high number. Among them, 18 were accepted (including 6 minor revisions) and 9 papers received a major revision decision. Out of the remaining rejected papers, 8 received a "reject and resubmit" decision. We received one SoK submission in 2023 (2), which got accepted after a minor revision. 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 "Cryptanalysis of HALFLOOP Block Ciphers: Destroying HALFLOOP-24" by Gregor Leander, Shahram Rasoolzadeh, and Lukas Stennes, and "Propagation of Subspaces in Primitives with Monomial Sboxes: Applications to Rescue and Variants of the AES" by Aurélien Boeuf, Anne Canteaut, and Léo Perrin.

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 Svetla Petkova-Nikova and Siemen Dhooghe for the organization of FSE 2024 in Leuven, Belgium. We would also like to thank Kevin McCurley and Kay McKelly for facilitation of remote participation. We are moreover thankful to Kevin for his help with the review process management system. We also would like to thank Anne Canteaut, 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 2024 Christina Boura
Kazuhiko Minematsu

Editorial Board

	Gaithersburg, United States
André Schrottenloher	Inria, Rennes, France
Yannick Seurin	Ledger, Paris, France
Meltem Sönmez Turan	National Institute of Standards and Technology (NIST), Gaithersburg, United States
François-Xavier Standaert	Université catholique de Louvain, Louvain-la-Neuve, Belgium
Ling Sun	Shandong University, Qingdao, China
Siwei Sun	University of Chinese Academy of Sciences, Beijing, China
Tyge Tiessen	Technical University of Denmark, Kongens Lyngby, Denmark
Yosuke Todo	NTT Social Informatics Laboratories, Tokyo, Japan
Aleksei Udovenko	University of Luxembourg, Esch-sur-Alzette, Luxembourg
Damian Vizár	Centre suisse d'électronique et de microtechnique (CSEM), Neuchâtel, Switzerland
Lei Wang	Shanghai Jiao Tong University, Shanghai, China
Qingju Wang	Telecom Paris, Institut Polytechnique de Paris, Palaiseau, France

External reviewers

Bishwajit Chakraborty
Chandranan Dhar
Pierre-Jean Spaenlehauer
Lars Tebelmann