IACR Transactions on Symmetric Cryptology
ISSN 2519-173X, Vol. 2022, No. 1, pp. 1–4. DOI:10.46586/tosc.v2022.i1.1-4

Preface to Volume 2022, Issue 1

Itai Dinur[1] and Bart Mennink[2]

[1] Ben-Gurion University, Beer Sheva, Israel
[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 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 advertize their results and engage in discussions on further work. In 2022, FSE was held during March 20-25, 2022 in Athens, Greece. However, due to the COVID-19 pandemic, the conference was organized in a different way than usual. Most importantly, the conference was held in a hybrid format, accommodating both in-person and online participation. In addition, as FSE 2021 was cancelled, part of the papers originally scheduled for FSE 2021 were postponed to FSE 2022. In detail, papers from the following six issues of ToSC have been presented at FSE 2022: 2020(4), 2021(1), 2021(2), 2021(3), 2021(4) and 2022(1). In addition to the scientific papers from the journal, FSE 2022 had two invited talks: Orr Dunkelman on optimizing cryptanalysis and Christian Rechberger on symmetric cryptography for new applications.

Table 1: Submission statistics for issues 2021(2), 2021(3), 2021(4), and 2022(1)

Volume (Issue)	Regular Submissions	Accepted (Minor Revision)	Major Revision	Decision Deferred	Reject and Resubmit	Addendum/ Errata
2021(2)	37	14(9)	0	0	6	0/0
2021(3)	44	7(5)	3	1	9	0/0
2021(4)	31	6(5)	3	0	9	0/0
2022(1)	46	9(5)	9	0	6	1/0

Table 1 gives the submission statistics for issues 2021(2), 2021(3), 2021(4), and 2022(1). For example, for Volume 2021, Issue 3, we received 44 regular submissions, out of which 7 were accepted (including 5 minor revisions) and 3 papers received a major revision decision. The decision for 1 submission was deferred to the next cycle. Out of the remaining rejected papers, 9 received a "reject and resubmit" decision. None of the (conditionally) accepted papers was an addendum or errata paper.

As it is tradition for FSE, the Editorial Board also selected a best paper, based on the scientific quality and contribution. This year the Editorial Board has decided to give the award to "Weak Keys in Reduced AEGIS and Tiaoxin" by Fukang Liu, Takanori Isobe, Willi Meier, and Kosei Sakamoto.

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 Christina Boura for the organization of FSE 2022 and her persistence during the pandemic, and to Kevin McCurley and Kay McKelly for making it possible to hold FSE 2022 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, Phil Hebborn, 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 2022

Itai Dinur
Bart Mennink

Editorial Board

Hadi Soleimany	Shahid Beheshti University, Teheran, Iran
Ling Song	Jinan University, Guangzhou, China
Siwei Sun	Chinese Academy of Sciences, Beijing, China
Yosuke Todo	NTT Secure Platform Laboratories, Tokyo, Japan
Aleksei Udovenko	CryptoExperts, Paris, France
Damian Vizár	Centre suisse d'électronique et de microtechnique (CSEM), Neuchâtel, Switzerland
Qingju Wang	University of Luxembourg, Luxembourg, Luxembourg
Friedrich Wiemer	cryptosolutions, Essen, Germany Robert Bosch, Stuttgart, Germany

External reviewers

Amit Singh Bhati

Ritam Bhaumik

Akinori Hosoyamada

Lukas Stennes

Mark Zhandry