IACR Transactions on Symmetric Cryptology
ISSN 2519-173X, Vol. 2019, No. 1, pp. 1–4. DOI:10.13154/tosc.v2019.i1.1-4

Preface to Volume 2019, Issue 1

Florian Mendel[1] and Yu Sasaki[2]

[1] Infineon Technologies, Neubiberg, Germany
florian.mendel@gmail.com
[2] NTT Secure Platform Laboratories, Tokyo, Japan
yu.sasaki.sk@hco.ntt.co.jp

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. Full papers are assigned to the members of the Editorial Board. 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. Detailed discussions among the reviewers lead to one of the following four decisions for each paper: ACCEPT, in which case the authors submit their final camera-ready manuscript after editorial corrections; ACCEPT with MINOR REVISION, which means that the authors revise their manuscript and go through one or more iterations and reviews of the manuscript until the comments have been addressed in a satisfactory way; MAJOR REVISION, which means that the authors are requested to make major changes to their manuscript before submitting again in one of the next rounds; and REJECT, which means that the manuscript is deemed to be not suitable for publication in ToSC. The last four issues we have tried to refine the method (new for a community used to only accept or reject decisions) and decide in a more fair way when to assign major revisions.

The review process shares with the high quality conferences that it is double-blind and adheres to a strict timing; but unlike a traditional conference, there are multiple submission deadlines per year. Each paper received at least three reviews; for submissions by Editorial Board members this was increased to at least four.

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 leads to an increased quality of the papers that are published.

The papers selected by the Editorial Board for publication in the last four issues were presented at the conference Fast Software Encryption (FSE). This gave the authors the opportunity to advertise their results and engage in discussions on further work. In 2019, FSE was held during March 25-28, 2019 in Paris, France. The papers presented at FSE 2019 appeared in ToSC Volume 2018, Issues 2-4 and Volume 2019, Issue 1. For Volume 2018, Issue 2, we received 25 submissions, out of which 7 were accepted, 2 of these after minor revisions; the number of papers that received a major revision decision was 5.

Published: 2019-03-19

For Volume 2018, Issue 3, we received 31 submissions, out of which 10 were accepted, 4 of these after minor revisions; the number of papers that received a major revision decision was 3. For Volume 2018, Issue 4, we received 41 submissions, out of which 8 were accepted, 5 of these after minor revisions; the number of papers that received a major revision decision was 5. For Volume 2019, Issue 1, we received 45 submissions, out of which 11 were accepted, 3 of these after minor revisions; the number of papers that received a major revision decision was 8.

Besides the 36 selected talks, the program included one invited talk by Gregor Leander on non-linear invariant attacks, María Naya-Plasencia on post-quantum security of symmetric-key cryptography, and Jian Guo on cryptanalysis of Keccak based constructions. The conference also featured a rump session, chaired by Pierre Karpman and Brice Minaud, with several short informal presentations. As it is tradition for FSE, the Editorial Board also selected a best paper, based on the scientific quality and contribution. The Editorial Board has decided to give the award to the paper by Léo Perrin entitled "Partitions in the S-Box of Streebog and Kuznyechik".

We would like to thank the authors of all submissions for contributing high quality submissions and giving us the opportunity to compile a good and diverse program. 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 would also like to thank the subreviewers for their efforts. We are profoundly indebted to the conference General Chair Jérémy Jean for his hard work to make the conference a success. We also would like to thank Anne Canteaut, Shai Halevi, Gregor Leander, and Friedrich Wiemer for their work and support. Finally, we would like to thank ANSSI, Thalès, INRIA, Ledger, ENS PSL, Pôle d'Excellence Cyber, CryptoExperts, Idemia, CyberCrypt, DIM RFSI, and Région Ile de France for their generous support of the conference.

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 2019

Florian Mendel
Yu Sasaki

Editorial Board

External reviewers

Christof Beierle
Lauren De Meyer
Johann Großschädl
Vasily Mikhalev
Kazuhiko Minematsu
Francois-Xavier Standaert
Aleksei Udovenko
Qingju Wang