IACR Transactions
ISSN 2519-173X, Vol. 2017, No. 1, pp. 1–3. DOI:10.13154/tosc.v2017.i1.1-3

Preface to Volume 2017, Issue 1

María Naya-Plasencia[1] and Bart Preneel[2]

[1] Inria, Paris, France
maria.naya_plasencia@inria.fr
[2] imec - Computer Security and Industrial Cryptography (COSIC) research group, Department of Electrical Engineering (ESAT), KU Leuven, Leuven, Belgium
bart.preneel@esat.kuleuven.be

As Co-Editors-in-Chief of the new journal IACR Transactions on Symmetric Cryptology (ToSC), we are pleased to present you the first issue of the 2017 volume. Following some other communities in computer science, ToSC is a new journal/conference hybrid that offers electronic publiation with gold open access (in our case the Creative Commons License CC-BY 4.0). The review procedures strictly adhere to the traditions of the journal world. Full papers are assigned to the members of the editorial board, who write detailed and careful reviews (in most cases without relying on subreviewers). Subsequently there is a rebuttal phase, during which authors get the opportunity to respond to the review comments. If necessary, the review process enables further interactions between the authors and the reviewers, mediated by the Co-Editors-in-Chief. After detailed discussions among the reviewers, one of the following four decisions is made 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 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 deadines per year. Each paper received at least three reviews; for submissions by Editorial Board members this was increased to five. The call for papers encourages the submission of long papers, which may take two rounds to review, and Systematization of Knowledge (SoK) papers, that review and contextualize the existing literature in a particular area. The papers selected for publication over the last year are presented at the conference Fast Software Encryption (FSE), which gives the opportunity to authors to advertise their results and engage in discussions on further work. The Editorial Board consisted of 37 members with broad research interests; they represent 18 countries.

Overall, we are very pleased with the quality and quantity of submissions, the extensive review reports written by the reviewers and the substantial efforts by the authors to further improve the quality of their work. We believe that the review process is productive and constructive and overall the process leads to an increased quality of the papers that are published.

The first edition of the conference FSE was held in Cambridge, UK in December 1993. It started with a small community of researchers fascinated by the move of cryptology from hardware to software implementations, which – together with the fast development of the Internet – would result in massive deployment of cryptography over the next decade. The focus was on practical constructions and cryptanalysis techniques for symmetric cryptology,

Published: 2017-03-08

as it was felt that other venues put more emphasis on public key cryptography and on theoretical work. An important characteristic of the conference was the publication of complete designs with detailed specifications, source code, and test values. Recently there is also increasing attention towards reproducibility of the results by making source code or tools for cryptanalysis available. Over the past 24 years, FSE has developed as the premier venue for research in symmetric cryptology. Since 2004, FSE was sponsored by the IACR (International Association for Cryptologic Research).

FSE 2017, the 24th conference on Fast Software Encryption, was held during March 6-8, 2017 in Tokyo, Japan. The papers presented at FSE appeared in ToSC Volume 2016, Issues 1 and 2 and Volume 2017, Issue 1. For Volume 2016, Issue 1, we received 28 submissions, out of which 9 were accepted, 2 of these after minor revisions; the number of papers that received a major revision decision was 12. For Volume 2016, Issue 2, we received 42 submissions, out of which 14 were accepted, 8 of these after minor revisions; the number of papers that received a major revision decision was 14. For Volume 2017, Issue 1, we received 55 submissions, out of which 22 were accepted, 13 of these after minor revisions; the number of papers that received a major revision decision was 7.

The Editorial Board has decided to give the best paper award to the paper by Colin Chaigneau, Thomas Fuhr, Henri Gilbert, Jeremy Jean and Jean-René Reinhard entitled *Cryptanalysis of NORX v2.0*.

The invited talks were delivered by Joan Daemen, who spoke on "Innovations in permutation-based encryption and/or authentication" and Shiho Moriai who shared with the audience her perspective on "Design, Analysis and Promotion of (Lightweight) Block Ciphers."

We would like to sincerely thank the authors of all submissions for contributing high quality submissions and giving us the opportunity to compile a strong and diverse program. Special thanks go to the Editorial Board members; we value their hard work and dedication to write careful and detailed reviews and to engage in interesting discussions. Many Editorial board members, whom we asked to serve as shepherds, spent additional time in order to help the authors improving their works. We would also like to thank the subreviewers for their efforts. We are greatly indebted to the conference General Chairs Tetsu Iwata and Shiho Moriai for their hard work to make the conference a success. We also would like to thank Gregor Leander, the first managing editor of ToSC, Anne Canteaut, the chair of the FSE Steering Committee, Gaëtan Leurent, the author of the IACR Transactions LaTeX class file, and Shai Halevi, the author of the IACR Web-Submission-and-Review software for their support and advice.

Finally, we would like to thank the International Exchange Program of National Institute of Information and Communications Technology (NICT), the Kayamori Foundation of Informational Science Advancement and the Support Center for Advanced Telecommunications Technology Research, Foundation (SCAT) for their generous support of the conference.

We hope that the papers in this volume of IACR Transactions on Symmetric Cryptology prove valuable for your research and professional activities and that ToSC will become the leading international venue where the best research on symmetric cryptology is published.

February 2017

María Naya-Plasencia
Bart Preneel

Editorial Board

External reviewers

Sebastian Faust	University of Bochum, Germany
Marco Martinoli	University of Bristol, Bristol, UK
Vasily Mikhalev	University of Mannheim, Germany