Preface to Volume 2020, Special Issue on Designs for the NIST Lightweight Standardisation Process

Itai Dinur\textsuperscript{1} and Gaëtan Leurent\textsuperscript{2}

\textsuperscript{1} Ben-Gurion University, Beer Sheva, Israel
\textsuperscript{2} Inria, Paris, France

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.

This special issue is dedicated to second-round candidates in NIST’s (National Institute of Standards and Technology) ongoing standardisation process for lightweight cryptography. This process started with a call for algorithms that received 57 submissions in February 2019, and 32 of them advanced to the second round in August 2019\textsuperscript{1}. One of the main goals of this issue was to encourage designers to submit high-quality schemes which might otherwise not have been formally published. It is the first special issue of ToSC dedicated to a specific topic.

As all ToSC issues, this special issue strives to maintain a high quality review process and 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.

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.

For this special issue we received 17 submissions, out of which 12 were accepted, 8 of those after a minor revision, and 1 of those after a major revision.

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.

\textsuperscript{1}https://csrc.nist.gov/Projects/lightweight-cryptography/round-2-candidates
We also would like to thank Anne Canteaut, Shai Halevi, Gregor Leander, Friedrich Wiemer, and Phil Hebborn 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.

May 2020

Itai Dinur
Gaëtan Leurent
Editorial Board

Frederik Armknecht  University of Mannheim, Mannheim, Germany
Tomer Ashur  KU Leuven, Leuven, Belgium
Subhadeep Banik  Ecole Polytechnique Federale de Lausanne (EPFL), Lausanne, Switzerland
Zhenzhen Bao  Nanyang Technological University (NTU), Singapore, Singapore
Christof Beierle  Ruhr University Bochum, Bochum, Germany
Christina Boura  University of Versailles, Versailles, France
Anne Canteaut  Inria, Paris, France
Joan Daemen  Radboud University, Nijmegen, The Netherlands
Patrick Derbez  University of Rennes, Rennes, France

Christoph Dobraunig  Radboud University, Nijmegen, The Netherlands
Orr Dunkelman  University of Haifa, Haifa, Israel
Maria Eichlseder  Graz University of Technology, Graz, Austria
Takanori Isobe  University of Hyogo, Kobe, Japan
Jérémy Jean  Agence Nationale de la Sécurité des Systèmes d’Information (ANSSI), Paris, France
Pierre Karpman  Université Grenoble Alpes, Grenoble, France
Stefan Kölbl  Google, Zurich, Switzerland
Virginie Lallemand  Centre National de la Recherche Scientifique (CNRS) Nancy, France

Jooyoung Lee  Korea Advanced Institute of Science and Technology (KAIST), Daejeon, South Korea
Stefan Lucks  Bauhaus-Universität Weimar, Weimar, Germany
Atul Luykx  Swirlds Inc., United States
Willi Meier  University of Applied Sciences and Arts Northwestern Switzerland (FHNW), Windisch, Switzerland
Florian Mendel  Infineon Technologies, Munich, Germany
Bart Mennink  Radboud University, Nijmegen, The Netherlands
Brice Minaud  Inria, Paris, France

Kazuhiko Minematsu  NEC, Kawasaki, Japan
Nicky Mouha  National Institute of Standards and Technology (NIST), Gaithersburg, United States
Samuel Neves  University of Coimbra, Coimbra, Portugal
Léo Perrin  Inria, Paris, France
Thomas Peyrin  Nanyang Technological University (NTU), Singapore, Singapore

Bart Preneel  KU Leuven, Leuven, Belgium
Yu Sasaki  NTT Secure Platform Laboratories, Tokyo, Japan
Hadi Soleimany  Shahid Beheshti University, Teheran, Iran
Ling Song  Nanyang Technological University (NTU), Singapore

Francois-Xavier Standaert  UCLouvain, Louvain-la-Neuve, Belgium
Siwei Sun  Chinese Academy of Sciences, Beijing, China
Elmar Tischhauser  Philipps-Universität Marburg, Marburg, Germany
Yosuke Todo  
NTT Secure Platform Laboratories, Tokyo, Japan

Gilles Van Assche  
STMicroelectronics, Diegem, Belgium

Damian Vizár  
Centre suisse d’électronique et de microtechnique (CSEM), Neuchâtel, Switzerland

**External reviewers**

Vasily Mikhalev