Preface to TCHES Volume 2021

Elke De Mulder[1] and Peter Schwabe[2,3]

[1] Rambus Cryptography Research
4453 North First Street, Suite 100
San Jose, CA 95134
USA

edemulder@rambus.com

[2] Max Planck Institute for Security and Privacy
Universitätsstraße 140
44799 Bochum
Germany

[3] Radboud University
Toernooiveld 212
6525 EC Nijmegen
The Netherlands

peter@cryptojedi.org

Having been established in 1999, the Cryptographic Hardware and Embedded Systems (CHES) conference is today the premier venue for research on both design and analysis of cryptographic hardware and software implementations. As an area conference of the International Association for Cryptologic Research (IACR), CHES bridges the cryptographic research and engineering communities, and attracts participants from academia, industry, government and beyond.

CHES 2021 was held as a virtual event on September 13–17, 2021 after careful discussion half a year prior to the conference dates about whether or not it would be realistic to hold an in-person event due to the ongoing COVID-19 pandemic. It was the second exclusively virtual and the twenty-third overall edition of the CHES conference.

Since 2018, CHES is run under a hybrid model as a mixture of journal publications and conference presentations. The papers constituting the CHES 2021 program were published in the IACR Transactions on Cryptographic Hardware and Embedded Systems (TCHES) Volume 2021, Issues 1, 2, 3 and 4 under a platinum open-access model. The journal is published by Ruhr-Universität Bochum; the managing director and publishing editor is Tim Güneysu.

This is the first year `HotCRP` was adopted as submission and review system. Despite some learning mistakes and per-deadline adjustments due to a still-evolving platform, the experiment was rather successful. One major feature still lacking from these review systems is the ability to deal with resubmissions and the administrative overhead it creates for the program chairs to keep track of previous reviewers and discussions.

To help the rebuttal process and aid the authors in deciding what to focus on while preparing their answer, we opted to include a section in the review form where reviewers could ask questions they deemed most important, with the goal to receive answers in the rebuttal.

Since it was an all-virtual and world-wide event, the conference presentations themselves were limited to five minutes; the full twenty-minute presentations were pre-recorded and made available online for people to enjoy at their own leisure.

IACR Transactions on Cryptographic Hardware and Embedded Systems ISSN 2569-2925, Vol. 2021, No. 1, pp. I–IV
DOI:10.46586/tches.v2021.i1.I-IV

Table 1: Submission statistics of TCHES Volume 2021.

	Issue 1	Issue 2	Issue 3	Issue 4
Number of new submissions	45	44	41	62
Number of major revisions from previous issues	4	7	24	10
Number of re-submissions from previous issues	3	1	4	5
Number of submissions (total)	52	52	69	77
Number of accepted submissions (total)	17	13	26	22
Number of accepted submissions (new only)	13	7	3	11
Acceptance rate	32.6%	25%	37.6%	28.5%

The submission statistics of TCHES Volume 2021 are summarized in Table 1. The four issues have received a total of 192 new submissions; counting the resubmissions, a total of 250 submissions were reviewed for this volume. Out of those 78 have been accepted, making a global acceptance rate of 31%. The higher acceptance rate is mostly due to the process of major revisions.

After voting, the Editorial Board conferred the CHES 2021 best paper award to *My other car is your car: Compromising the Tesla Model X keyless entry system* by Lennert Wouters, Benedikt Gierlichs and Bart Preneel. The program included two invited talks: *From CHERI to Arm Morello: Architectural Support for Memory Protection and Software Compartmentalization* by Robert Watson (University of Cambridge) and *Hardware for privacy engineering* by Carmela Troncoso (EPFL).

New this year was the addition of an optional artifact review and archiving process for accepted papers which was deftly chaired and organized by Douglas Stebila from the University of Waterloo. The main goal was to to ensure functionality and reusability of artifacts. All about this process can be read in a separate preface. We sincerely hope that this evaluation of artifacts will continue to be part of the TCHES/CHES publication model.

Acknowledgments. Creating a journal and conference is a labor-intensive task and a lot of minds and hands have to come together and put in effort to make it happen. We would like to thank all the parties involved. We would like to thank our sponsors for their generous contribution: Rambus, CryptoExperts, NXP, SciEngines, Infineon, Open Security Research and Qualcomm. We would like to extend thanks to the general chairs Liji Wu, Guoqiang Bai, Zhe Liu, and Junfeng Fan. A special shout-out goes to Douglas Stebila who took on the daunting task to organize the first ever CHES artifact review process. Two hundred fifty submissions, spread over four deadlines resulted in a big workload. The result achieved could not have been possible without the dedication and professionalism of the Editorial Board members and the external reviewers. Without the help of Kevin McCurley and Kay McKelly who administer and maintain not only the `HotCRP` software, but take care of all the technical aspects of running a virtual conference, neither the journal, nor the conference would have happened. The publication of TCHES was supported by Tim Güneysu in the role of Managing Editor and Markus Krausz for the practical issues; constituent papers all used a LaTeX style originally authored by Gaëtan Leurent. A special thanks also goes to the CHES Steering Committee for support and advice during these unprecedented time and the hard decision to once more have a virtual-only conference. Last, but not least we are indebted to the authors of all the submissions. Without those, there would be no CHES in the first place.

September 2021

Elke De Mulder
Peter Schwabe

Editorial Board

External Reviewers