Journal of Cryptographic Engineering (2023) 13:389–390
https://doi.org/10.1007/s13389-023-00338-w

EDITORIAL

The ASHES 2021 special issue at JCEN

Chip-Hong Chang[1] · Stefan Katzenbeisser[2] · Debdeep Mukhopadhyay[3] · Ulrich Rührmair[4,5]

Received: 24 September 2023 / Accepted: 25 September 2023 / Published online: 18 November 2023

Abstract
This brief editorial gives a short, two-page overview of the ASHES 2021 workshop. It shall serve as an introduction for this special issue at JCEN.

Keywords Secure hardware · Physical attacks · Defenses

1 Editorial

It is our pleasure to introduce readers to this special ASHES 2021 issue at the Journal of Cryptographic Engineering.

Let us start by some general remarks on the underlying workshop series. The ASHES workshop on "**A**ttacks and **S**olutions in **H**ardwar**E** **S**ecurity" welcomes **any** theoretical and practical submissions on hardware security. This obviously includes any works on attacks, solutions, countermeasures, classifications, formalizations, proofs, and implementations in the field of hardware security. But besides such mainstream research, ASHES also puts a particular focus on new or emerging scenarios: Examples include the internet of things (IoT), nuclear weapons inspections, arms control, automotive security, consumer and public infrastructure security, supply chain security, anti-counterfeiting, or non-electronic security systems. In order to cover this broad spectrum, the workshop hosts four different paper categories: Apart from regular and short papers, this includes works that systematize and structure a certain area (so-called **S**ystematization **o**f **K**nowledge (SoK) papers, as well as "**W**ild-**a**nd-**C**razy" (WaC) papers, which shall distribute seminal ideas at an early conceptual stage.

This special ASHES 2021 issue at the Journal of Cryptographic Engineering (JCEN) now covers selected papers from the fifth edition of the workshop, which took place on November 19, 2021, in Seoul (South Korea), as a one-day post-conference satellite workshop of ACM CCS. The ASHES 2021 morning session hosted a keynote by Ruby Lee (Princeton) on *"Speculative Execution Attacks and Hardware Defenses"*. The afternoon featured a keynote by Farinaz Koushanfar (UC San Diego) on *"Machine Learning on Encrypted Data: Hardware to the Rescue"*. In the technical program, eleven papers addressed the various research areas being served by ASHES. They were distributed over four technical sessions throughout the day: PHYSICAL ATTACKS (I); SECURE HARDWARE DESIGN; WILD-AND-CRAZY; and PHYSICAL ATTACKS (II). A full program is available from http://asheswork shop.org/workshop-program-2021 to interested readers.

After the workshop, the authors of said eleven papers were invited to submit extended versions to this special issue at JCEN. We are happy to state that almost all authors followed our invitation. After a thorough review process, seven extended versions were accepted for publication and are now presented in this special issue. These seven papers cover a broad spectrum of topics within hardware security: They range from various new and exciting side channel attacks and countermeasures to key encapsulation mechanisms, and cover the security of FCMW radar just as well as hardware security verification. We are glad to present such a diverse mixture and program to readers in this special issue.

✉ Ulrich Rührmair
ruehrmair@ilo.de

Chip-Hong Chang
ECHChang@ntu.edu.sg

Stefan Katzenbeisser
stefan.katzenbeisser@uni-passau.de

Debdeep Mukhopadhyay
debdeep@cse.iitkgp.ac.in

[1] NTU Singapore, Singapore, Singapore

[2] Universität Passau, Passau, Germany

[3] IIT Kharagpur, Kharagpur, India

[4] TU Berlin, Berlin, Germany

[5] University of Connecticut, Storrs, USA

The ASHES workshop in every single year clearly is a team effort. In this context, we would like to express our sincere gratitude to various colleagues involved in the workshop's organization. Let us start with our program committee members, for all their hard work in reading, evaluating, and commenting on the original submissions. (A full list can be found under http://ashesworkshop.org/committees-2021).

Furthermore, we are strongly indebted to various other esteemed colleagues associated with ASHES: Domenic Forte, our publicity chair; Francesco Regazzoni, our proceedings chair; and Yuan Cao, our web chair. This, of course, also includes all ASHES steering committee (SC) members, who have been driving and supporting the workshop over the years: Chip- Hong Chang, NTU Singapore (SC Co-Chair); Srini Devadas, MIT; Marten van Dijk, CWI and VU Amsterdam; Çetin Kaya Koç, UC Santa Barbara; Farinaz Koushanfar, UC San Diego; Ulrich Rührmair, TU Berlin and U Connecticut (SC Chair); Ahmad-Reza Sadeghi, TU Darmstadt; Francois-Xavier Standaert, UC Louvain; Mark M. Tehranipoor, U Florida; and Ingrid Verbauwhede, KU Leuven.

Last, but certainly not least, a very special thanks goes to Çetin Kaya Koç, the editor in chief of JCEN, for inviting ASHES to periodic, annual special issues at JCEN since 2019.

But for now, we hope readers will enjoy the current special issue—and look forward to seeing you at some future edition of the ASHES workshop!

Author contributions All authors contributed to the underlying special issue by managing the review of (individually assigned parts of) the submissions.

Funding Open Access funding enabled and organized by Projekt DEAL.

Declarations

Conflict of interest The authors declare no conflict of interest.

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.