Journal of Cryptographic Engineering (2022) 12:369–370
https://doi.org/10.1007/s13389-022-00300-2

EDITORIAL

The ASHES 2020 special issue at JCEN

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

Published online: 12 September 2022

Abstract
This editorial provides its readers with a brief introductory overview of the ASHES workshop series in general, and of this special ASHES 2020 issue at the Journal of Cryptographic Engineering (JCEN) in particular.

Keywords ASHES workshop · Hardware security · Editorial · ACM CCS

Introducing readers to this special ASHES 2020 issue at JCEN is both a great pleasure and privilege indeed. Let us start by some general remarks on the underlying workshop series. Founded in 2017, the ASHES workshop welcomes *any* theoretical and practical articles in the field of hardware security. This certainly includes all works on attacks, solutions, countermeasures, proofs, classifications, formalizations, and implementations. Besides said mainstream research, ASHES also puts particular emphasis on emerging scenarios: Examples include the Internet of things (IoT), nuclear weapons inspections, arms control, automotive security, consumer security, infrastructure security, supply chain security, anti-counterfeiting, or non-electronic security systems. 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 *"Systematization of Knowledge (SoK)"* papers), as well as *"Wild-and-Crazy (WaC)"* papers, which shall distribute seminal ideas at an early conceptual stage.

This special ASHES 2020 issue at JCEN now covers selected papers from the fourth edition of the workshop, which took place on November 13, 2020, in Orlando (USA), as a one-day post-conference satellite workshop of ACM CCS. The morning session of the workshop hosted a keynote by Mark M. Tehranipoor (U Florida) entitled "*The Pursuit of Happiness: Establishing Hardware Root-of-Trust for Cyber Security."* The afternoon featured a keynote of Çetin Kaya Koç (UC Santa Barbara) on "*Formidable Challenges in Hardware Implementations of Fully Homomorphic Encryption Functions for Applications in Machine Learning."* Furthermore, eleven scientific papers addressed the various active research fields at ASHES throughout the workshop's technical program. They were grouped in four sessions: *"PUFs and Beyond," "Side Channels: Attacks and Defenses," "Fault Attacks and Cryptographic Hardware Design,"* and *"Hardware and Systems Security."*

After the workshop, all authors of these eleven papers were invited to submit extended versions to this special ASHES issue at JCEN. The main requirement was that 25% new material should be added to the new versions. We are happy to state that almost all authors followed our invitation. Submissions were then evaluated in a standard procedure via external reviewers. Any conflicts of interest (COIs) of reviewers and editors were identified and handled rigorously in this process; all editors were completely isolated from the review processes of any of their COI papers. Eventually, seven extended versions were accepted for publication, and are now presented in this special issue.

We would also like to take this opportunity to express our sincere gratitude to various colleagues involved in the ASHES workshop and in this special issue.

Firstly, to our program committee members at ASHES 2020, for all their hard work in reading, evaluating, and commenting on the original submissions:

- Tolga Arul, University of Passau
- Aydin Aysu, North Carolina State University

✉ Ulrich Rührmair
ulrich.ruehrmair@lmu.de

1 NTU Singapore, Singapore, Singapore

2 University of Passau, Passau, Germany

3 LMU Munich, Munich, Germany

4 University of Connecticut, Storrs, USA

5 Worcester Polytechnical Institute, Worcester, USA

- Lejla Batina, Radboud University
- Yuan Cao, Hohai University
- Rajat Subhra Chakraborty, IIT Kharagpur
- Chip Hong Chang, Nanyang Technological University
- Jean-Luc Danger, Télécom ParisTech
- Ghada Dessouky, TU Darmstadt
- Giovanni Di Crescenzo, Perspecta Labs
- Wieland Fischer, Infineon Technologies
- Domenic Forte, University of Florida
- Michael Franz, University of California
- Helena Handschuh, Rambus
- Daniel Holcomb, UMass Amherst
- Chenglu Jin, New York University
- Ramesh Karri, Polytechnic Institute of NYU
- Ryan Kastner, University of California San Diego
- Stefan Katzenbeisser, University of Passau
- Juliane Krämer, TU Darmstadt
- Markus Kuhn, University of Cambridge
- Itamar Levi, UC Louvain
- Roel Maes, Intrinsic-ID
- Avi Mendelson, Technion
- Ahmad Moghimi, Worcester Polytechnic Institute
- Debdeep Mukhopadhyay, IIT Kharagpur
- David Naccache, ENS Paris
- Makoto Nagata, Kobe University
- Maire O'Neill, Queen's University Belfast
- Alex Orailoglu, University of California San Diego
- David Oswald, University of Birmingham
- Jeyavijayan Rajendran, Texas A&M
- Ulrich Rührmair, LMU Munich and U of Connecticut
- Markku-Juhani Saarinen, PQShield Ltd.
- Patrick Schaumont, Worcester Polytechnic Institute
- Jean-Pierre Seifert, TU Berlin
- Sergei Skorobogatov, University of Cambridge
- Mostafa Taha, Carleton University
- Shahin Tajik, University of Florida
- Ingrid Verbauwhede, Katholieke Universiteit Leuven
- Claire Vishik, Intel Corporation (UK)
- Nils Wisiol, Freie Universität Berlin
- Fan Zhang, Zhejiang University

Secondly, we are certainly no lesser indebted to various other colleagues associated with ASHES in different ways: To our publicity chair Domenic Forte (U Florida); our proceedings chair Francesco Regazzoni (U Amsterdam/USI Lugano); our web chair Yuan Cao (Hohai U); and, of course, all (other) steering committee members, who have thankfully been driving and supporting the workshop over the years: Srini Devadas (MIT), Marten van Dijk (CWI Amsterdam/U Connecticut), Çetin Kaya Koç (UC Santa Barbara), Farinaz Koushanfar (UC San Diego), 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 feature annual special issues at JCEN in the first place.

But for now, we hope readers will find this special issue from 2020 inspiring—and look forward very much to meeting you in person at some future edition of the ASHES workshop.

Funding Open Access funding enabled and organized by Projekt DEAL.