Journal of Cryptographic Engineering (2021) 11:199–200
https://doi.org/10.1007/s13389-021-00270-x

REGULAR PAPER

The ASHES 2019 special issue at JCEN

Chip-Hong Chang[1] · Daniel E. Holcomb[2] · Ulrich Rührmair[3,4] · Patrick Schaumont[5]

Received: 30 July 2021 / Accepted: 30 July 2021 / Published online: 22 August 2021

Abstract
This brief editorial gives a short, two-page overview of the ASHES 2019 workshop. It shall serve as an introduction for this special issue at JCEN.

Keywords ASHES workshop · Hardware security · Editorial · ACM CCS

Editorial and some brief guiding comments

It is our pleasure to introduce readers to this special ASHES 2019 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" generally welcomes any theoretical and practical submissions on hardware security. This includes all works on attacks, solutions, countermeasures, proofs, classifications, formalizations, and implementations. 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 infrastructure security, supply chain security, 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 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 2019 issue at the Journal of Cryptographic Engineering (JCEN) now covers selected papers from the third edition of the workshop, which took place on November 15, 2019, in London (UK), as a one-day post-conference satellite workshop of ACM CCS. The morning session of ASHES 2019 hosted a keynote by Francois-Xavier Standaert (UC Louvain) entitled "Towards an Open Approach to Side-Channel Resistant Authenticated Encryption." The afternoon featured a keynote of Ross Anderson (Cambridge University) on "30 Years of Tamper Resistance." In the technical program, 11 papers addressed the various research areas being served by ASHES. They were presented within four technical sessions throughout the day: Physical-layer security and PUFs; side channels and fault attacks; reverse engineering and trusted manufacturing; and FPGA-security and memory attacks.

After the workshop, authors of said 11 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, eight extended versions were accepted for publication and are now presented in this special issue.

In this context, we are very grateful to various people that made the workshop and this special issue possible. This starts with our program committee members at ASHES, for all their hard work in reading, evaluating, and commenting the original submissions:

– Aydin Aysu, North Carolina State University
– Lejla Batina, Radboud University
– Swarup Bhunia, University of Florida

✉ Ulrich Rührmair
ruehrmair@ilo.de

Chip-Hong Chang
ECHChang@ntu.edu.sg

Daniel E. Holcomb
dholcomb@umass.edu

Patrick Schaumont
pschaumont@wpi.edu

[1] NTU Singapore, Singapore, Singapore

[2] University of Massachusetts Amherst, Amherst, USA

[3] LMU Munich, Munich, Germany

[4] University of Connecticut, Storrs, USA

[5] Worcester Polytechnical Institute, Worcester, USA

- Rajat Subhra Chakraborty, IIT Kharagpur
- Nicolas T. Courtois, University College London
- Jean-Luc Danger, Télécom ParisTech
- Giovanni Di Crescenzo, Perspecta Labs
- François Dupressoir, University of Surrey
- Wieland Fischer, Infineon Technologies
- Domenic Forte, University of Florida
- Siddharth Garg, New York University
- Helena Handschuh, Rambus
- Tsung-Yi Ho, National Tsing Hua University
- Daniel Holcomb, UMass Amherst
- Chris Kim, University of Minnesota
- Michel Kinsy, Boston University
- Markus Kuhn, University of Cambridge
- Itamar Levi, UCL University
- Roel Maes, Intrinsic ID
- Yiorgos Makris, University of Texas at Dallas
- Debdeep Mukhopadhyay, IIT Kharagpur
- Saibal Mukhopadhyay, Georgia Inst. of Technology
- Maire O'Neill, Queen's University Belfast
- Alex Orailoglu, University of California San Diego
- David Oswald, University of Birmingham
- Daniel Page, University of Bristol
- Sébastien Philippe, Harvard University
- Nguyen Phuong Ha, University of Connecticut
- Jeyavijayan Rajendran, Texas A&M
- Ulrich Rührmair, LMU Munich and U Connecticut
- Patrick Schaumont, Virginia Tech
- Tobias Schneider, NXP Semiconductors
- Jean-Pierre Seifert, TU Berlin
- Sergei Skorobogatov, University of Cambridge
- Jakub Szefer, Yale University
- Shahin Tajik, University of Florida
- Ingrid Verbauwhede, KU Leuven
- Fan Zhang, Zhejiang University

Furthermore, we are strongly indebted to various other esteemed colleagues associated with ASHES: Domenic Forte, our publicity chair; Francesco Regazzoni, our proceedings chair; Yuan Cao, our web chair; and, of course, all steering committee members, who have been driving and supporting the workshop over the years.

Last, but certainly not least, a very special thanks goes to Cetin Kaya Koc, the editor in chief of JCEN, for inviting ASHES to periodic, annual special issues at JCEN from this year onward!

But for now, we hope readers will enjoy this special issue from 2019—and look forward to seeing you at some future edition of the ASHES workshop!

Funding Open Access funding enabled and organized by Projekt DEAL.