November 30, 2023
Copenhagen, Denmark

Association for Computing Machinery

Advancing Computing as a Science & Profession

ASHES '23

Proceedings of the 2023 Workshop on
Attacks and Solutions in Hardware Security

Sponsored by:

ACM SIGSAC

General Chairs:

Chip Hong Chang, (NTU, Singapore)

Ulrich Rührmair, (LMU, Munich and U Connecticut)

Association for
Computing Machinery

Advancing Computing as a Science & Profession

The Association for Computing Machinery
1601 Broadway, 10th Floor
New York, NY 10019-7434

ISBN: 979-8-4007-0262-4

Additional copies may be ordered prepaid from:

ACM Order Department
PO Box 30777
New York, NY 10087-0777, USA

Phone: 1-800-342-6626 (USA and Canada)
+1-212-626-0500 (Global)
Fax: +1-212-944-1318
E-mail: acmhelp@acm.org
Hours of Operation: 8:30 am – 4:30 pm ET

Printed in the USA

ASHES 2023 – Welcome Message

It is our great pleasure to welcome you to the **Seventh Workshop on Attacks and Solutions in Hardware Security 2023 (ASHES 2023)**, a post-conference satellite workshop of the ACM Conference on Computer and Communications Security 2023 (CCS 2023).

ASHES deals with **all** theoretical and practical aspects of hardware security and welcomes any contributions to this area. Besides being a mainstream platform for disseminating fundamental research, the workshop also encourages and promotes emerging and new ideas. This includes diverse topics such as physical attacks, secure hardware designs and implementations, lightweight secure systems, post-quantum security, as well as emerging topics at the intersection of nanotechnology and security, such as physical unclonable functions (PUFs). The workshop also puts a particular focus on recent applications like the internet of things, automotive security, smart homes, or pervasive and wearable computing. ASHES thereby aims at giving researchers and practitioners a unique opportunity to share their perspectives.

In order to account for hardware security as a rapidly developing discipline, ASHES routinely offers four categories of submission:

- Full papers;
- Short papers;
- Systematization of Knowledge *(SoK)* papers, which structure or survey a certain subarea within hardware security;
- Wild and Crazy *(WaC)* papers, whose aim is to distribute a promising and potentially seminal research idea at an early stage to the community.

In 2023, our call for papers attracted 33 submissions overall. One submission fell into the wild-and-crazy paper category; the rest were regular full (27) and short papers (4). Geographically, the submissions came from the USA (16), Europe (13) and Asia (4), and the different co-authors of submissions were associated with institutions in the US (55), Europe (39), China (6), India (5), Iran (4), Japan (3), Vietnam (2) and South Korea (1) .

Twelve submissions were accepted as papers to the program, amounting to an acceptance rate of 36%. These twelve accepted papers were hosted in five technical sessions with the following topics:

- Side-Channel Attacks (3 papers)
- Novel Attacks and Implementations (3 papers)
- Artificial Intelligence and Side-Channel Attacks (2 papers)
- Fault Attacks (2 papers)
- Reverse Engineering (2 papers)

We hope that this established a nice and diverse balance between all different themes offered by the ASHES call for papers.

Said twelve technical papers were complemented by two carefully chosen keynotes from leading experts in their areas, to which we would particularly draw the readers' attention. In alphabetical order:

- Ravi Pappu (formerly MIT, now Apeiron Labs): *Physical Unclonable Functions: The First Fifty Years*
- Claire Vishik (formerly Fellow and Group CTO at Intel, now co-founder and CTO of a stealth startup): *In Search of Trust: 30 Years of Evolution of Trusted Computing and Hardware Security*

Any further details on ASHES, its scope, its committees, and its program can be found under www.ashesworkshop.org.

We would like to stress that organizing and setting up ASHES was clearly a team effort. First of all, we are much indebted to all authors for submitting their ideas and insights to the workshop. Secondly, we are no less grateful to the program committee, who worked hard in reviewing papers and providing feedback for authors, and to the two PC chairs Lejla Batina and Domenic Forte, who did an outstanding job. Also the web chair, Yuan Cao, and the publications chair, Francesco Regazzoni, deserve special mentioning and our deep gratitude. Nothing less holds for the publicity chairs Naghmeh Karimi, who greatly supported us in rising the submissions. We furthermore would like to thank the hosting conference, CCS 2023, and all its organizers, including the CCS workshop co-chairs, for their enduring and very strong support. Special thanks go to the two keynote speakers, Ravi Pappu and Claire Vishik, for agreeing to share their wisdom with us! Finally, we would like to thank and mention all steering committee (SC) members of ASHES in alphabetical order, namely Chip- Hong Chang (SC co-chair), Srini Devadas, Marten van Dijk, Çetin Kaya Koç Farinaz Koushanfar, Ulrich Rührmair (SC chair), Ahmad-Reza Sadeghi, Francois-Xavier Standaert, Mark Tehranipoor, and Ingrid Verbauwhede, for their key role in ensuring the workshop's success.

We hope that you will find the ASHES program inspiring and thought-provoking, and that the workshop will provide you with the opportunity to share ideas with fellow researchers and practitioners from other institutions worldwide. We also hope that ASHES will continue to grow and to establish itself within the highly competitive landscape of existing hardware security venues as a recurring workshop, after its first seven editions!

Domenic Forte
ASHES 2023 Program Co-Chair
University of Florida, USA

Lejla Batina
ASHES 2023 Program Co-Chair Radboud
University, NL

Chip Hong Chang
ASHES 2023 Workshop Co-Chair
NTU, Singapore

Ulrich Rührmair
ASHES 2023 Workshop Co-Chair
TU Berlin, Germany, &
University of Connecticut, USA

Francesco Regazzoni
ASHES 2023 Workshop Publication Chair
University of Amsterdam, The Netherlands, &
Università della Svizzera italiana, Switzerland

Table of Contents

Workshop Short Paper

ASHES 2023 Workshop Organization

General Chairs: Chip Hong Chang, NTU Singapore
Ulrich Rührmair, LMU Munich and U Connecticut

Program Chairs: Lejla Batina, Radboud U
Domenic Forte, U of Florida

Proceedings Chair: Francesco Regazzoni, U Amsterdam and U Svizzera italiana

Publicity Chair: Naghmeh Karimi, University of Maryland

Web Chair: Yuan Cao, Hohai University

Steering Committee: Chip Hong Chang, NTU Singapore, co-chair
Srini Devadas, MIT
Marten van Dijk, CWI Amsterdam and U Connecticut
Çetin Kaya Koç, UC Santa Barbara
Farinaz Koushanfar, UC San Diego
Debdeep Mukhopadhyay, IIT Kharagpur
Ulrich Rührmair, LMU and U Connecticut, chair
Ahmad-Reza Sadeghi, TU Darmstadt
Francois-Xavier Standaert, UC Louvain
Mark Tehranipoor, U Florida
Ingrid Verbauwhede, KU Leuven

Program Committee: Anupam Chattopadhyay, NTU
Avi Mendelson, Technion
Aydin Aysu, North Carolina State University
Avani Dave,Intel
Calvin Deutschbein, Willamette University
Chenglu Jin, CWI Amsterdam
Chester Rebeiro, IIT Madras, India
Chip Hong Chang, Nanyang Technological University
Claire Vishik, Intel Corporation, UK
Cheng Gongye,Northeastern University
Daniel Holcomb, UMass Amherst
David Oswald, University of Birmingham
Debapriya Basu Roy, IIT Kharagpur
Debdeep Mukhopadhyay, IIT Kharagpur, India
Domenic Forte, University of Florida
Elena Dubrova, KTH Royal Institute of Technology
Fatemeh Ganji, Worcester Polytechnic Institute
Francesco Regazzoni, U Amsterdam and U Svizzera italiana
Fan Zhang,Zhejiang University
Glenn Cowan, Concordia University

Program Committee, continued:

Haoting Shen, Zhejiang University
Helena Handschuh, Rambus
Itamar Levi, UCL university, Belgium
Jean-Luc Danger, Télécom ParisTech, CNRS/LTCI
Jeyavijaya Rajendran, Texas A&M
Ileana Buhan,Radboud University, Nijmegen
Lejla Batina,Radboud University, Nijmegen
Lois Orosa, ETH Zurich
Lukasz Chmielewski,Brno university, Czech Republic
Maria Mushtaq,Institut Télécom/Télécom ParisTech, CNRS/LTCI
Michael Zuzak,Rochester Institute of Technology
Michael Hutter,PQ Shield
Mulong Luo,Cornell University
Makoto Nagata, Kobe University
Markku-Juhani Saarinen, PQShield Ltd.
Mostafa Taha, Carleton University
Naghmeh Karimi, University of Maryland, UMBC
Nele Mentens,KU Leuven
Rajat Subhra Chakraborty, IIT Kharagpur
Sara Achour, Stanford University
Sarani Bhattacharya, imec Belgium
Sayandeep Saha, IIT Kharagpur
Sergei Skorobogatov, University of Cambridge
Seetal Potluri,SUNY, Albany
Shahin Tajik, Worcester Polytechnic Institute
Shuwen Deng, Yale University
Stefan Katzenbeisser, University of Passau
Sheng Wei ,Rutgers University
Sandhya Koteshwara,IBM
Soheil Salehi,University of Arizona
Takeshi Sugawara,The University of Electro-Communications
Tolga Arul, University of Passau
Ulrich Rührmair, LMU Munich and U Connecticut
Vincent Immler, Oregon State University
Walter Krawec, University of Connecticut
Wei Hu, Northwestern Polytechnical University & University of California, San Diego
Wen Wang, Intel Labs
Wenjie Xiong, Virginia Tech
Wieland Fischer, Infineon Technologies
Xiaolin Xu,Northeastern University
Yang Li,Nanjing University of Aeronautics and Astronautics
Zheng Yue,Nanyang Technological University / CUHKSZ

Additional reviewers:

Anirban Chakraborty
Kevin Gubbi
Martin Thompson
Nimish Mishra
Shuvodip Maitra
Siddhartha Chowdhury
Suvadeep Hajra

Sponsor: