



## ASHES 2023 – CALL FOR PAPERS & PARTICIPATION

We are happy to announce the **Seventh Workshop on Attacks and Solutions in Hardware Security (ASHES 2023)**, a post-conference satellite workshop of **ACM CCS 2023**, one of the premier computer security conferences, on Nov. 30, 2023, in Copenhagen, Denmark.

**ASHES deals with any aspects of hardware security, including both theory and practice, and welcomes any contributions in this area.** Besides traditional topics, it also invites novel methods and emerging applications: This includes new attack vectors, novel designs and materials, lightweight security primitives, nanotechnology, and PUFs, as well as the internet of things, automotive security, smart homes, or pervasive and wearable computing.

**More specifically, topics of interest include, but are not limited to:**

- Fault injection and countermeasures
- Side channels and countermeasures
- Hardware Trojans and countermeasures
- Tamper sensing and tamper protection
- New physical attack vectors or methods
- Biometrics
- Secure sensors and sensor networks
- Device fingerprinting and hardware forensics
- Emerging computing technologies in security
- Lightweight hardware solutions
- Lightweight implementation of cryptographic and security primitives
- Security of reconfigurable and adaptive hardware
- Post-quantum security
- New designs and materials in hardware security
- Nanophysics and nanotechnology in hardware security
- PUFs and new/emerging variants thereof
- Secure implementation and design of security primitives
- Scalable hardware solutions for many players/endpoints
- Item tagging, secure supply chains, and product piracy
- Hardware security and machine learning
- Hardware security in emerging application scenarios
- Hardware-based information leakage in the cloud
- Electronic voting machines
- Hardware security in mobile platforms
- Architectural factors in hardware security, isolation versus encryption
- Secure hardware for multiparty computation
- Secure hardware in intellectual property protection and content protection
- Integration of hardware roots of trust and PUF
- Quality metrics for secure hardware
- Conformance and evaluation of secure hardware
- Formal treatments, formal proofs, or standardization/categorization of hardware-related techniques
- Hardware security in the internet of things

**ASHES hosts four different categories of papers:** Classical full papers; short papers; wild and crazy (WaC) papers (whose purpose is rapid dissemination of promising, potentially game-changing novel ideas); and systematization of knowledge (SoK) papers (which overview, structure, and categorize a certain subarea). **All accepted ASHES papers are part of the ACM Digital Library, and will also be invited as extended versions to the ASHES special issue at the Journal of Cryptographic Engineering (JCEN) at Springer.**

ASHES will also feature **two invited keynotes** by **Ravikanth Pappu (formerly MIT/Apeiron Labs)** and **Claire Vishik (Intel)**.

### Committees

#### Steering Committee

Chip Hong Chang (NTU), Co-Chair  
Sriini Devadas (MIT)  
Marten van Dijk (CWI & UConn)  
Çetin Kaya Koç (UC Santa Barbara)  
Farinaz Koushanfar (UC San Diego)  
Debdeep Mukhopadhyay (IIT Kharagpur)  
Ulrich Rührmair (UConn & LMU), Chair  
Ahmad-Reza Sadeghi (TU Darmstadt)  
Francois-Xavier Standaert (UC Louvain)  
Mark M. Tehranipoor (U Florida)  
Ingrid Verbauwhede (KU Leuven)

#### Workshop Chairs

Chip Hong Chang (NTU Singapore)  
Ulrich Rührmair (UConn & LMU)

#### PC Chairs

Lejla Batina (Radboud U)  
Domenic Forte (U Florida)

#### Proceedings/Publicity Chair

Francesco Regazzoni (U Lugano)  
Naghme Karimi (U Maryland)

#### Web Chair

Yuan Cao (Hohai U)

### Important Dates

#### Paper submission deadline:

**July 16, 2023, 23:59:59 EDT**

#### Acceptance notification:

August 21, 2023

#### Camera-ready versions:

September 5, 2023

#### Workshop Date:

November 30, 2023