ASHES 2017 — ATTACKS AND SOLUTIONS IN HARDWARE SECURITY
Nov. 3, 2017, Dallas, USA

CALL FOR PAPERS

We are happy to announce the **First Workshop on Attacks and Solutions in Hardware Security (ASHES 2017)**, a post-conference satellite workshop of CCS 2017, taking place on **Nov. 3, 2017,** in Dallas, Texas, USA (see http://ashesworkshop.org).

ASHES deals with any aspects of hardware security, and welcomes any contributions in this area. It particularly highlights emerging techniques and methods as well as recent application areas within the field. This includes new attack vectors, novel designs and materials, lightweight security primitives, nanotechnology, and PUFs on the methodological side, as well as the internet of things, automotive security, smart homes, pervasive and wearable computing on the applications side.

Specific topics of interest include, but are not limited to:

- Tamper sensing and tamper protection
- Physical attacks (fault injection, side-channels, etc.),
- including new attack vectors or attack methods
- Biometrics and hardware security
- Physical unclonable functions
  (and new/emerging variants thereof)
- Device fingerprinting and hardware forensics
- Item tagging, secure supply chains and product piracy
- Use of emerging computing technologies in security
  (including quantum techniques)
- New designs and materials for secure hardware
- Nanophysics and nanotechnology in hardware security
- Hardware Trojans and countermeasures

- Lightweight security solutions, primitives and protocols
- Secure and efficient hardware implementation of cryptographic primitives
- Security of reconfigurable and adaptive hardware platforms
- Sensors and sensor networks
- Hardware security in emerging application scenarios: Internet of Things, smart home, automotive, wearable computing, pervasive and ubiquitous computing, etc.
- Scalable hardware solutions that work for particularly large numbers of players/endpoints
- Formal treatments, proofs, standardization, or categorization of the area
  (incl. surveys and systematization of knowledge papers)

ASHES hosts four different categories of papers:

- **Classical full and short papers**.
- **Wild and crazy (WaC) papers**, whose purpose is rapid dissemination of promising, potentially game-changing novel ideas.
- **Systematization of knowledge (SoK) papers**, which overview, structure, and/or categorize a certain subarea of hardware security.

Please see http://ashesworkshop.org/call-for-papers for additional details.

The workshop will include three invited keynotes by Srini Devadas (MIT), Ulfar Erlingsson (Google), and Ahmad-Reza Sadeghi (TU Darmstadt). Please visit http://ashesworkshop.org/keynotes for further information.

Committees

Steering Committee

Chip Hong Chang (NTU Singapore)

Marten van Dijk (U Connecticut)

Farinaz Koushanfar (UC San Diego)

Ulrich Rührmair (U Bochum, Founder)

Mark Tehranipoor (U Florida)

Program Chairs

Chip Hong Chang (NTU Singapore)

Ulrich Rührmair (U Bochum)

Publication Chair

Wei Zhang (HKUST Hong Kong)

Web Chair

Yuan Cao (NTU Singapore)

Important Dates

Paper submission deadline:	August 4, 2017
Acceptance notification:	September 4, 2017
Camera-ready deadline:	September 17, 2017
Workshop date:	**November 3, 2017**

ashesworkshop.org