



# ASHES 2017—Workshop on Attacks and Solutions in Hardware Security

Chip Hong Chang  
NTU Singapore  
ECHChang@ntu.edu.sg

Marten van Dijk  
University of Connecticut  
vandijk@engr.uconn.edu

Farinaz Koushanfar  
UC San Diego  
farinaz@ucsd.edu

Ulrich Rührmair  
Ruhr-University Bochum  
ruehrmair@ilo.de

Mark Tehranipoor  
University of Florida  
tehranipoor@ece.ufl.edu

## ABSTRACT

The workshop on “**attacks and solutions in hardware security**” (ASHES) deals with all aspects of hardware security, including any recent attacks and solutions in the area. Besides mainstream research in hardware security, it also covers new, alternative or emerging application scenarios, such as the internet of things, nuclear weapons inspections, satellite security, or consumer and supply chain security. It also puts some focus on special purpose hardware and novel methodological solutions, such as particularly lightweight, small, low-cost, and energy-efficient devices, or even non-electronic security systems. Finally, ASHES welcomes any theoretical works that systematize and structure the area, and so-called “Wild-and-Crazy” papers that describe and distribute seminal ideas at an early conceptual stage to the community.

## CCS Concepts/ACM Classifiers

- CCS Concept: Hardware Security

## Keywords

Hardware security; secure design; special purpose hardware; hardware attacks; internet of things; non-electronic security hardware; emerging application scenarios for security hardware

## 1 INTRODUCTION AND MOTIVATION

As predicted by Gartner in 2015, there will be around 21 billion hardware devices connected in the IoT by 2020, creating a spending of about 3,000 billion dollars per year. This makes the IoT and associated hardware security questions clearly one of the most massive and impactful endeavors of this century.

At the same time, the development of suitable hardware strategies seems to lag behind the actual spread of the IoT.

Permission to make digital or hard copies of part or all of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for third-party components of this work must be honored. For all other uses, contact the Owner/Author.

*CCS'17, October 30–November 3, 2017, Dallas, TX, USA.*

© 2017 Copyright is held by the owner/author(s).

ACM ISBN 978-1-4503-4946-8/17/10.

<https://doi.org/10.1145/3133956.3137049>

While the security community has long recognized that many of the established, classical recipes do not transfer easily (or not at all) to hardware in an IoT-setting, no fully convincing substitute strategies have been developed yet. This leads to a host of novel questions, which cannot be addressed by existing means and methods alone. One particular scientific challenge lies in the unprecedented threat landscape of the IoT, which will connect billions of pervasive, low-cost devices with no strong tamper-protection or even computational resources on board. Particularly pressing questions in this context include:

- How can we get individual cryptographic keys into billions of low-cost hardware devices?
- How can we securely identify low-cost hardware over digital channels, e.g., systems without digital signal processors or devices merely powered by scavenged energy?
- How can we protect against tampering and side-channels in low-cost hardware?
- How can we remotely verify the functionality and integrity of connected IoT-devices?
- How can we establish the long-term confidentiality of communications with resource-constrained hardware?
- How can we protect the IoT and its hardware against malware (viruses, Trojan horses, etc.) and network attacks?
- How can we enable secure physical data storage in lightweight hardware systems?
- How can we preserve the privacy of users in pervasive IoT-scenarios?

The purpose of this workshop is to foster solutions for these and other impending issues on hardware security, in particular with hindsight to new methods and application scenarios such as the IoT. It shall provide the CCS-community with a dedicated, specialized forum for this type of research. It is thereby meant not only to cover mainstream hardware security research, but also to support novel research and methods at an early stage, fostering innovation in the area.

## 2 TOPICS

ASHES deals with the entire range of established, mainstream hardware security research, but particularly tries to foster novel and innovative approaches, as well as emerging application areas.

This includes, but is 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)

## 3 PAPER CATEGORIES

To account for the special scope of the workshop, and for the particular nature of hardware security as a rapidly developing discipline, the workshop offers four different categories of papers:

- **Full papers**, with up to 10 pages in ACM double column format (including references and appendices), and a 25 min presentation timeslot at the workshop (including questions).
- **Short papers**, with up to 6 pages in ACM double column format (including references and appendices), and a 15 min presentation timeslot at the workshop (including questions).

- **Wild and Crazy (WaC) papers**, with 3 to 6 pages in ACM double column format, with additional appendices and references of up to 6 pages, and 15 min presentation timeslot at the workshop (including questions). WaC papers are meant to target groundbreaking new methods and paradigms for hardware security. Their focus lies on novelty and potential impact, and on the plausibility of their argumentation, but not on a full demonstration or complete implementation of their ideas. They are reviewed and assessed as such. Wild and crazy papers must bear the prefix “WaC:” in their title from the submission onwards.
- **Systematization of Knowledge (SoK) papers**, with up to 12 pages in ACM double column format (including appendices and references), and a 25 min presentation timeslot at the workshop (including questions). SoK papers shall evaluate, systematize, and contextualize existing knowledge. They should serve the community by fostering and structuring the development of a particular subarea within hardware security. Ideally, but not necessarily, they might provide a new viewpoint on an established, important subarea, support or challenge long-standing beliefs with compelling evidence, or present a convincing new taxonomy. They will be reviewed and assessed as such. Systematization of knowledge papers must bear the prefix “SoK:” in the title from the submission onwards.

## 4 PROGRAM

- 8:50 am - 9:00 am: *Welcome*
- 9:00 am - 10:00 am: *Invited Talk: Srinivas Devadas (MIT)*  
Secure Hardware and Cryptography: Contrasts, Synergies and Challenges
- 10:00 am - 10:25 am: *Coffee Break*
- 10:25 am - 11:25 pm: *Invited Talk: Ahmad-Reza Sadeghi (TU Darmstadt):*  
Hardware-Assisted Security: Promises, Pitfalls and Opportunities
- 11:25 am - 12:15 pm: *Session No. 1: Solutions in Hardware Security*
  - Giovanni Di Crescenzo (Vencore Labs), Jeyavijayan Rajendran (UT Dallas), Ramesh Karri (NYU), Nasir Memon (NYU) and Yevgenij Dodis (NYU): Boolean Circuit Camouflaging: Cryptographic Models, Limitations, Provable Results, and a Random Oracle Realization
  - Charles Suslowicz, Archanaa S Krishnan and Patrick Schaumont (all Virginia Tech): Optimizing Cryptography in Energy Harvesting Applications

- 12:15 pm – 2:00 pm: Lunch, Socializing
- 2:00 pm – 3:00 pm: *Invited Talk:*  
*Ulfar Erlingsson (Google)*  
Data-driven Software Security and its  
Hardware Support
- 3:00 pm – 3:30 pm: *Coffee Break*
- 3:30 pm - 4:10 pm: *Session No 2: WaC&SoK*
  - Yan Michalevsky and Yonatan Winetraub  
(both Stanford):  
WaC: SpaceTEE - Secure and Tamper-Proof  
Computing in Space using CubeSats
  - Hoda Maleki, Reza Rahaeimehr and Marten  
van Dijk (all University of Connecticut):  
SoK: A survey of Clone Detection approaches  
in RFID-based supply chains
- 4:10 pm – 5:00 pm: *Session No. 3:  
Attacks in Hardware Security*
  - Lars Tebelmann, Michael Pehl and Georg  
Sigl (all TU München):  
EM Attack on BCH-based Error Correction  
for PUF-based Key Generation
  - Varnavas Papaioannou and Nicolas Courtois  
(both University College London):  
On the Feasibility and Performance of  
Rowhammer Attacks

## ACKNOWLEDGMENTS

Ulrich Rührmair acknowledges support by the German Ministry of Science and Education within the project “PICOLA”.