

# HOST 2017: IEEE International Symposium on Hardware-Oriented Security and Trust

May 1-5, 2017, The Ritz-Carlton Tysons Corner, McLean, VA

**HOST 2017**  
<http://hostsymposium.org>

## General Chair

Swarup Bhunia, University of Florida

## Program Chair

Ryan Kastner, UC San Diego

## Vice-Program Chair

Gang Qu, University of Maryland

## Finance Chair

Yier Jin, University of Central Florida

## Publicity Chair

Qiaoyan Yu, Univ. of New Hampshire

## Local Arrangements Chair

Hassan Salmani, Howard University

## Tutorial Chair

Domenic Forte, University of Florida

## Registration Chair

Ioannis Savidis, Drexel University

## Panel Chair

Saverio Fazzari, Booz Allen Hamilton

## Industrial Liaison Chair

Mark Tehranipoor, Univ. of Florida  
Farinaz Koushanfar, UC San Diego

## Asia-Pacific Liaison

R. S. Chakraborty, IIT Kharagpur

## Hardware Demo Chair

Jim Plusquellic, Univ. of New Mexico

## A/V Chair

Avesta Sasan, George Mason University

## Web Chair

Wei Hu, UC San Diego

## Call for Papers

*IEEE International Symposium on Hardware Oriented Security and Trust (HOST)* aims to facilitate the rapid growth of hardware-based security research and development. HOST highlights new results in the area of hardware and system security. Relevant research topics include techniques, tools, design/test methods, architectures, circuits, and applications of secure hardware. **HOST 2017** invites original contributions related to, but not limited by, the following topics.

- **Hardware Trojan attacks, detection techniques and countermeasures**
- **Hardware techniques to facilitate software and/or system security**
- **Hardware-based security primitives (PUFs, RNGs)**
- **FPGA and system-on-chip (SoC) security**
- **Side-channel attacks and protection**
- **Security, privacy, and trust protocols**
- **Metrics, policies, and standards related to hardware security**
- **Hardware IP trust (watermarking, metering, trust verification)**
- **Trusted manufacturing including split manufacturing and 3D ICs**
- **Security analysis and protection of Internet of Things (IoT)**
- **Secure and efficient implementation of crypto algorithms**
- **Reverse engineering and hardware obfuscation**
- **Supply chain risks mitigation (e.g., counterfeit detection & avoidance)**
- **Hardware tampering attacks and protection**
- **Applications of hardware security to secure system development**

You can register and submit your paper at: <https://easychair.org/conferences/?conf=host2017>. The page limit is 6 pages, double column, IEEE format, with a minimum font size of 10 points. Submissions are anonymous and must not identify the authors, directly or indirectly, anywhere in the manuscript.

Students can participate in a hardware demo session by submitting a 1-page proposal describing the research and features to be demonstrated on an FPGA or other hardware platform. Please upload your proposal to EasyChair by Feb. 1, 2017.

A best paper award will be given to paper whose first author is a full-time student. A best presentation award will be given to a speaker who is a full-time student. Travel grants are available for graduate and undergraduate students.

## IMPORTANT DATES:

Registration of Title + Abstract:	<b>November 15, 2016</b>
Submission of Paper:	<b>November 22, 2016</b>
Tutorial Proposal:	<b>December 1, 2016</b>
Notification of Acceptance:	<b>January 31, 2017</b>
Camera-ready Version:	<b>February 28, 2017</b>
Hardware Demo Proposal:	<b>February 1, 2017</b>

## Technical Program: Ryan Kastner

Tel: +1 (858) 534-8908

E-mail: [kastner@ucsd.edu](mailto:kastner@ucsd.edu)

## General Information: Swarup Bhunia

Tel: +1 (352) 392-5989

E-mail: [swarup@ece.ufl.edu](mailto:swarup@ece.ufl.edu)

## HOST 2017 sponsors:



IEEE  
Computer Society  
Technical Committee on  
Security and Privacy