

General Chair

S. Bhunia, U. of Florida

General Co-Chair

T-Y. Ho, National Tsing Hua U.

Program Chair

Y. Jin, U. of Central Florida

Vice-program Chair

O. Sinanoglu, NYU Abu Dhabi

Finance Chair

G. Qu, U of Maryland

Publicity Chair

D. Forte, U. of Florida

R. Chakraborty, IIT Kharagpur

S. Narasimhan, Intel

Local Arrangements Chair

C-M. Cheng, National Taiwan U.

Y-Y. Liu, Yuan-Ze U.

Registration Chair

C-Y. Lee, National Tsing Hua U.

Panel Chair

S. Fazzari, DARPA

Tutorial Chair

Y. Liu, Tsinghua U.

Industrial Liaison

M. Tehranipoor, U. of Florida

Publications Chair

C-H. Chang, NTU

Steering Committee

M. Tehranipoor, U. of Florida (Chair)

Y. Jin, U. of Central Florida

S. Bhunia, U. of Florida

F. Koushanfar, UCSD

G. Qu, U. of Maryland

O. Sinanoglu, NYU Abu Dhabi

T-Y. Ho, National Tsing Hua U.

H. Yang, Tsinghua U.

J. Plusquellic, UNM

Call for Papers

Hardware has long been viewed as a trusted party supporting the whole computer system and is often treated as an abstract layer running instructions passed through the software layer. Historically, cybersecurity community believed that the integrated circuit (IC) supply chain is well protected. However, the IC supply chain, which is now spread around the globe, has become more vulnerable to attacks than before. The heavy reliance on third-party resources/services breeds security concerns and invalidates the illusion that attackers cannot easily access the isolated IC supply chain. Formal methods have been proven to be effective in security verification on hardware code. Trustworthy hardware is also under development for the construction of the root-of-trust. The intrinsic properties of existing and emerging devices, MOSFET, memristor, spintronics, etc. are leveraged for security primitives and applications. Another trend in the hardware security area is the development of security enhanced hardware infrastructure for system level protection. The goal is to provide a fully operational software and hardware platform that ensures secure design, manufacturing, and deployment of modern computer systems.

IEEE Asian Hardware Oriented Security and Trust Symposium (AsianHOST) aims to facilitate the rapid growth of hardware security research and development in Asia and South Pacific areas. AsianHOST 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. **AsianHOST 2016** invites original contributions related to, but not limited by, the following topics.

- **Hardware Trojan attacks and detection techniques**
- **Side-channel attacks and countermeasures**
- **Metrics, policies, and standards related to hardware security**
- **Secure system-on-chip (SoC) architecture**
- **Security rule checks at IP, IC, and System levels**
- **Hardware IP trust (watermarking, metering, trust verification)**
- **FPGA security**
- **Trusted manufacturing including split manufacturing, 2.5D, and 3D ICs**
- **Emerging nanoscale technologies in hardware security applications**
- **Security analysis and protection of Internet of Things (IoT)**
- **Cyber-physical system (CPS) security and resilience**
- **Reverse engineering and hardware obfuscation at all levels of abstraction**
- **Supply chain risks mitigation including counterfeit detection & avoidance**
- **Hardware techniques that ensure software and/or system security**
- **Analysis of real attacks and threat evaluation**

To present at the symposium, submit an Acrobat (PDF) version of your paper on the symposium submission website (<https://easychair.org/conferences/?conf=asianhost2016>). The page limit is 6 pages, double column, IEEE format, with a minimum font size of 10 points. Submissions must be anonymous and must not identify the authors, directly or indirectly, anywhere in the manuscript.

SCHEDULE:

Registration of Title + Abstract:

August 8, 2016

Submission of Paper:

August 15, 2016

Notification of Acceptance:

September 22, 2016

Camera-ready Version:

October 15, 2016

Technical Program: Y. Jin

U. of Central Florida

Tel: +1 (407) 823-5321

E-mail: yier.jin@eecs.ucf.edu

General Information: S. Bhunia

U. of Florida

Tel: +1 (352) 392-5989

E-mail: swarup@ece.ufl.edu

For students:

- **Best paper award** for a paper whose first author is a full-time student at the submission time.

2016 sponsors:



IEEE
Computer Society
Technical Committee on
Security and Privacy