Asian Hardware Oriented Security and Trust Symposium

December 11-13, 2026, IIT Kharagpur, India

asianhost.org

General Chairs
Debdeep Mukhopadhyay (IIT Kharagpur, India)
Partha Pratim Chakrabarti (IIT Kharagpur, India)

Program Chairs
Sarani Bhattacharya (IIT Kharagpur, India)
Anupam Chattopadhyay (NTU, Singapore)

Finance Chairs
Yier Jin, University of Science and Technology of China

Publication Chairs
Dr. Sreyosi Bhattacharyya

PhD Forum and Special Sessions Chair
Debayan Das (IISc, India)
Chandan Karfa (IIT Guwahati, India)

Sponsors

Call for Papers

Historically, cybersecurity community believed that the underlying hardware is secure and trustworthy. However, the globalization of the IC supply chain invalidates the illusion of an isolated and trusted supply chain; the wide connection of computing devices also exposes new and powerful attack surfaces. Heavy reliance on third-party resources/services renders hardware security and trust a concern. With the advances in artificial intelligence and internet of things, the threat landscape is evolving with relentless new problems and challenges awaiting the hardware security community to address. Multi-disciplinary research and multi-pronged approaches are sought for the development of fully operational software and hardware platforms with enhanced security targeting different phases in the entire IC life cycle.

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 domain of hardware and system security. Relevant research topics include techniques, tools, design/test methods, architectures, circuits, and applications of secure hardware. **AsianHOST 2026** invites original contributions related to, but not limited by, the following topics:

- **Hardware-intrinsic security primitives (e.g., PUF and TRNG)**
- **Architectural and microarchitectural attacks and defenses**
- **Secure system-on-chip (SoC) architecture**
- **Trusted platform modules and hardware virtualization**
- **Side-channel attacks and countermeasures**
- **Hardware Trojan attacks and detection techniques**
- **Security analysis and protection of Internet of Things (IoT)**
- **Hardware IP core protection and trust for consumer electronics systems and IoT**
- **Security and trust of machine learning and artificial intelligence**
- **Automobile, self-drive and autonomous vehicle security**
- **5G and physical layer security**
- **Hardware-assisted cross-layer security**
- **Cyber-physical system (CPS) security and resilience**
- **Metrics, policies, and standards related to hardware security**
- **Security verification at IP, IC, and system levels**
- **Reverse engineering and hardware obfuscation**
- **Supply chain risks mitigation including counterfeit detection & avoidance**
- **Trusted manufacturing including split manufacturing, 2.5D, and 3D ICs**
- **Emerging nanoscale technologies in hardware security applications**
- **Cybersecurity Solutions for AI and LLM**

To contribute to the symposium, submit a PDF version of your paper on the symposium submission website (https://easychair.org/conferences/?conf=asianhost2026). The page limit is 6 pages, double column, IEEE format, with a minimum font size of 9 pts (preferably 10 pts). Submissions must be anonymous and must not identify the authors, directly or indirectly, anywhere in the manuscript. In addition to the full papers, AsianHOST 2026 will accept selected submissions as four-page short papers to be presented in a poster session. Accepted papers will be submitted for inclusion into IEEE Xplore subject to meeting IEEE Xplore's scope and quality requirements. Best paper award will be presented to the authors of a paper whose first author is a full-time student at the submission time. Selected papers will be invited to submit to a special issue in ACM TECS (approval pending).

Important Dates:

Submission of Paper:	**July 14, 2026, AOE**
Notification of Acceptance:	**September 4, 2026**
Camera-ready Version:	**October 30, 2026**

Contact Information:

Technical Program:
Anupam Chattopadhyay
NTU, Singapore
E-mail: anupam@ntu.edu.sg

General Information:
Debdeep Mukhopadhyay
IIT Kharagpur, India
Email: debdeep@cse.iitkgp.ac.in