CADforAssurance Panel 5: Hardware Assurance vs. AI: Friend or Foe?

Assurance of electronic hardware against diverse security and trust issues has become a complex, challenging problem. On one hand, explosion of design complexity demand a highly sophisticated design and verification process. On the other, hardware life cycle for both ASIC and COTS (e.g., FPGA, microcontroller, etc.) components, increasingly involve multitude of trust issues, requiring new thinking in system design and verification that can address the underlying lack of trust. AI techniques have shown great promises in mitigating these issues – from rapid exploration of viable attack space to detection of anomalous design artifacts. While the power of AI/ML is poised to make transformative impact on hardware assurance, the research community has also identified assurance issues with AI/ML hardware themselves. In particular, their vulnerability against malicious manipulations, information leakage, and other attacks have created major concerns. This panel will examine the crucial challenge of hardware assurance in the modern supply chain ecosystem, evolving role of AI/ML in hardware assurance, and discuss their interdependence/conflicts.

MODERATORS

Swarup Bhunia
U. of Florida

Ankur Srivastava
U. of Maryland

PANELISTS

Mike Borza
Synopsys

Vivian Kammler
Sandia National Lab

Brian Knight
Microsoft

Len Orlando
AFRL

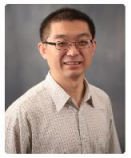
Sam Weber
ONR

Aug 12, FRIDAY, 11:00 AM – 12:30 PM EST

Register (for FREE) TODAY!

Organizers

JV Rajendran



Gang Qu

Tsung-Yi Ho

Yier Jin