IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems

Special Issue on

Hardware Oriented Security and Trust: Threats, Countermeasures and Design Tools

Call for Papers

IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems (TCAD) is announcing a special issue on "*Hardware Oriented Security and Trust: Threats, Countermeasures and Design Tools*", which invites top papers accepted to the **2019 Asian Hardware Oriented Security and Trust Symposium (AsianHOST 2019**, http://asianhost.org/2019/**)** for extension and also calls for original research papers through public contributions.

The purpose of this special issue is to provide the targeted readers with the new advances and challenges in hardware security research and development. Topics of interest include discoveries of emerging security threats that are encountered by the hardware design and supply chain, demonstration of the most recent hardware security attacks and mitigations, as well as new security protection techniques and design methodologies that help to thwart these threats. Relevant topics include, but are not limited to, the following:

• Architectural and micro-architectural attacks and defenses
• Secure system-on-chip (SoC) architectures
• Side-channel attacks and countermeasures
• Hardware Trojan attacks and detection techniques
• IP core protection for consumer electronics systems and IoT
• Security and trust of machine learning and artificial intelligence
• Automobile, self-drive and autonomous vehicle security
• 5G, physical layer and wireless security
• Hardware-assisted cross-layer security
• Cyber-physical system (CPS) security
• Metrics, policies, and standards related to hardware security
• Security verification at IP, IC, and system levels
• Hardware IP trust (watermarking, fingerprinting, metering, trust verification)
• 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
• Emerging nanoscale technologies in hardware security applications
• Hardware-intrinsic security primitives (Physical unclonable functions, true random number generator, etc.)
• Trusted platform modules and hardware virtualization

Paper Submission

All submissions must be made through the IEEE TCAD online paper submission system at https://mc.manuscriptcentral.com/tcad. Detailed submission instructions can be found at https://ieee-ceda.org/publication/tcad-publication/tcad-paper-submission

Submission Deadline: **March 1st, 2020**

Guest Editors

Chip Hong Chang, School of Electrical & Electronic Engineering, Nanyang Technological University, Singapore (Email: ECHChang@ntu.edu.sg)

Swarup Bhunia, Department of Electrical & Computer Engineering, University of Florida, USA (Email: swarup@ece.ufl.edu)

Ryan Kastner, Department of Computer Science and Engineering, University of California San Diego, USA (Email: kastner@ucsd.edu)

Hai Li, Electrical and Computer Engineering, Duke University, USA (Email: hai.li@duke.edu)

Anirban Sengupta, Computer Science & Engineering, Indian Institute of Technology Indore, India (Email: asengupt@iiti.ac.in)

Wei Hu, School of Automation, Northwestern Polytechnical University, China (Email: weihu@nwpu.edu.cn)

Editor in Chief

Rajesh Gupta, Department of Computer Science and Engineering, University of California San Diego, USA (Email: gupta@eng.ucsd.edu)

Deputy Editor in Chief

Xin Li, Electrical and Computer Engineering, Duke University, USA (Email: hai.li@duke.edu) (Email: xinli.ece@duke.edu)