IEEE Transactions on Circuits and Systems I: Regular Papers

CALL FOR PAPERS

Special Issue on
Emerging Hardware Security and Trust Technologies

Hardware security and trust have become a pressing issue during the last two decades due to the globalization of the semiconductor supply chain and ubiquitous network connection of computing devices. In addition to software, hardware circuits and systems are now an attractive attack surface for launching powerful cross-layer security attacks, allowing attackers to infer secret information, hijack control flow, compromise system root-of-trust, steal intellectual property, and fool machine learners. Hardware security threats can arise during various stages of the entire circuit life cycle, ranging from specification, design to fabrication and even recycling, which make the hardware security uniquely challenging.

The purpose of this special issue is to effectively convey the most up-to-date topics in the hardware security community. Topics of interest for this special issue lies in the introduction of most recent security attacks and threat models that are discovered in the hardware design and supply chain, emerging applications, as well as circuit theory, design methodology, design tools and implementations that help to thwart these threats. We sincerely hope not only this special issue can be a valuable reference for the target readers and researchers in the hardware security community, but also can motivate researchers in circuit and system design and in emerging technologies such as 5G/6G, IoT and artificial intelligence, to consider the new challenges and opportunities of incorporating an additional dimension of security into robust circuit and system design, testing, verification and implementation.

Hardware security is a fashionable research area in both industry and academy. Its scope is consistently growing. This special issue will include papers from extended version of AsianHOST 2023 and it also opens to public submissions related to emerging hardware security and trust technologies.

Authors are invited to submit Regular papers following the IEEE Transactions on Circuits and Systems I: Regular Papers (TCAS-I) guidelines within the scope of this Special Issue. Topics in scope for “Emerging Hardware Security and Trust Technologies” include (but are not limited to):

- Hardware-intrinsic security primitives (e.g., PUF and TRNG)
- Architectural and microarchitectural attacks and defenses
- Secure system-on-chip (SoC) architecture
- Post quantum cryptography (PQC) implementation
- 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

Submission Guidelines:

Manuscripts should be prepared following the TCAS-I Information for Authors, which can be found at https://ieee-cas.org/publication/TCAS-I/tcas-i-manuscript-submission-guide
and submitted through IEEE author portal at https://ieee.atyponrex.com/journal/tcas1
Please choose the option "Special Issue on Emerging Hardware Security and Trust Technologies" in your submission.

Please note that papers submitted to TCAS-I are expected to be typically of 9-11 pages and no more than 14 pages in length in the two-column IEEE Transactions format. Please read the Information for Authors regarding mandatory overlength page charges beyond 11 pages.

Please be aware that the submitted paper will undergo the standard review process to ensure that all the contributions meet the high standards of the Journal. In this regard, if a conference paper has been previously published, your submission to this special issue must be a significantly more complete version of your conference contribution with appropriate addition of experimental data or other relevant verification. As a rule of thumb, you should add at least 70% more unpublished technical material. When submitting the extended journal version of your conference paper, you must disclose the original conference paper and attach a letter explicitly highlighting the additional contributions of the TCAS-I paper relative to the original conference paper.

The tentative schedule of the review process is as follows:

• Paper submission	May 01, 2024
• First round review due	Jun 15, 2024
• Revised manuscript submission	Jul 30, 2024
• Second round review due	Aug 20, 2024
• Second (minor) revised paper submission	Sep 10, 2024
• Guest editor final recommendation	Sep 30, 2024
• Final accepted paper submission due	Oct 15, 2024
• Expected inclusion in issue	Dec 31, 2024

Guest Editors:

Qiang Liu, Tianjin University, China
Weiqiang Liu, Nanjing University of Aeronautics and Astronautics, China
Chongyan Gu, Queen's University Belfast, U.K
Reza Azarderakhsh, Florida Atlantic University, U.S.A.

Prof. Xinmiao Zhang,
Associate Editor-in-Chief, IEEE Transactions on Circuits and Systems-I: Regular Papers