IEEE Embedded Systems Letters

Special Issue on Hardware Security for post-CMOS technologies

Call for Papers

IEEE EMBEDDED SYSTEMS LETTERS seeks to provide a forum of quick dissemination of research results in the domain of embedded systems with a target turnaround time of no more than three months. The journal is currently published quarterly consisting of new, short and critically refereed technical papers. This special issue is about attacks and defenses of the emerging technology based embedded systems. The special issue covers several aspects ranging from technology, circuits, architecture, automation and vulnerability investigations.

Modern societies are heavily dependent on electronic systems. Especially with the emergence of IoT and advanced embedded electronic devices, such as mobile computers, wearables, and smartwatches, personalization is apparent. The rise of the electronic device jungle has provided a large attack surface to the bad actors to manipulate hardware and information processed. The attacks can significantly affect the three foundational aspects of secure hardware: confidentiality, integrity, and availability. Those cornerstones of hardware security in embedded systems are in danger of physical and remote attacks by adversaries during different periods of their design and life cycles. Depending on the attack, the countermeasure can also be innovative and wide in range. The future of computing is expected to be in the nano-structures composed of different types of devices and emerging technologies such as ReRAMs, biosensors, MRAM, and others. In this special issue, we cover attacks and countermeasures in future-generation embedded systems that utilize their nano-structure composition for security.

Topics:

- Design, implementation, and testing of Physically Unclonable Functions, True Random Number Generators, Memory Hash Functions, and others, using post-CMOS technologies for embedded systems
- Security of neuromorphic accelerators
- Fault attacks on emerging technology-based embedded systems
- Device, technology, and circuit-level attacks and countermeasures for emerging technologies
- Security-by-design for neuromorphic computing using emerging technologies
- Side-channel attacks and defenses on post-CMOS/emerging technologies for IoT and automotive embedded systems
- System-level security through technological innovations in emerging technologies
- Covert channels and information leakage in emerging technologies and systems
- Security of edge devices using neuromorphic/emerging technologies
- Attacks and countermeasures on embedded machine learning platforms with emerging technologies
- methodologies and tools for hardware security by design
- Quantum-safe cryptography using emerging technologies
- Methodologies and tools for hardware security-by-design in emerging technology based systems

Schedule:

- **Submission deadline:** September 5, 2021

Manuscripts should adhere to the technical requirement for IEEE Embedded Systems Letters (IEEE ESL). To guarantee a fast review and publication process; we require a strict page limit for all papers in this journal, without any exception. This strict limit is 4 pages, and the format is required to be exactly as stated in this guideline. Submitted papers to the special issue must conform to the technical requirements of IEEE ESL. They should be original and unpublished.

Guest Editors:

Farhad Merchant, RWTH Aachen University, Germany
Email: farhad.merchant@ice.rwth-aachen.de
Shahar Kvatinsky, Technion – Israel Institute of Technology, Israel
Email: shahar.kvatinsky@ee.technion.ac.il
Rainer Leupers, RWTH Aachen University, Germany
Email: leupers@ice.rwth-aachen.de