Proposal for a Special Issue in IEEE Embedded Systems Letter

Title: Hardware Security for post-CMOS technologies

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

Motivation:

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: July 30, 2021
   Author notification: September 25, 2021
   Revised manuscript submission: October 25, 2021
   Final manuscript submission: November 25, 2021
Potential contributors:

Akash Kumar (TU Dresden), Debdeep Mukhopadhyay (IIT Kharagpur), Stephan Menzel (FZ Juelich), Vikas Rana (FZ Juelich), Said Hamdioui (TU Delft), Mottaqiallah Taouil (TU Delft), Onur Mutlu (ETH Zurich), Luca Benini (ETH Zurich), Frank Altmann (Fraunhofer IMWS, Halle), Tolga Arul (University of Passau), Christian Boit (TU Berlin), Ralf Brederlow (TU Munich), Lucas Di (University of Duisburg-Essen), Rolf Drechsler (University of Bremen), Nan Du (TU Chemnitz), Thomas Eisenbarth (University of Luebeck), Tim Guenesu (Ruhr University Bochum), Jens Trommer (NaMLab GmbH), Swarup Bhunia (University of Florida), Mark Tehranipoor (University of Florida), Ujjwal Guin (Auburn University), Maire O'Neill (Queen's University, Belfast), Anupam Chattopadhyay (NTU, Singapore), Krishnendu Chakrabarty (Duke University), Ramesh Karri (New York University), Mehdi Tahoori (KIT)

Short bio of the guest editor(s):

Farhad Merchant received his Ph.D. from the Indian Institute of Science, Bangalore (India), in 2016. His Ph.D. thesis title was "Algorithm-Architecture Co-design for Dense Linear Algebra Computations." He received the DAAD fellowship during his Ph.D. He worked as a postdoctoral research fellow at Nanyang Technological University (NTU), Singapore, from March 2016 to December 2016. In December 2016, he moved to Corporate Research in Robert Bosch in Bangalore as a Researcher, where he worked on numerical methods for ordinary differential equations. He joined Institute for Communication Technologies and Embedded Systems, RWTH Aachen University, in December 2017 as a postdoctoral research fellow in the Chair for Software for Systems on Silicon. Farhad is the recipient of the HiPEAC technology transfer award in 2019.

Shahar Kvatinsky is an Associate Professor at the Andrew and Erna Viterbi Faculty of Electrical Engineering, Technion – Israel Institute of Technology. Shahar received a B.Sc. degree in Computer Engineering and Applied Physics and an MBA degree in 2009 and 2010, respectively, both from the Hebrew University of Jerusalem and the Ph.D. degree in Electrical Engineering from the Technion – Israel Institute of Technology in 2014. From 2006 to 2009, he worked as a circuit designer at Intel. From 2014 and 2015, he was a post-doctoral research fellow at Stanford University. Kvatinsky is an editor of Microelectronics Journal and has been the recipient of numerous awards: 2020 MDPI Electronics Young Investigator Award, 2019 Wolf Foundation’s Krill Prize for Excellence in Scientific Research, 2015 IEEE Guillemin-Cauer Best Paper Award, 2015 Best Paper of Computer Architecture Letters, Viterbi Fellowship, Jacobs Fellowship, ERC starting grant, the 2017 Pazy Memorial Award, the 2014 and 2017 Hershel Rich Technion Innovation Awards, 2013 Sanford Kaplan Prize for Creative Management in High Tech, 2010 Benin prize, and seven Technion excellence teaching awards. His current research is focused on circuits and architectures with emerging memory technologies and design of energy-efficient architectures.

Rainer Leupers received the M.Sc. (Dipl.-Inform.) and Ph.D. (Dr. rer. nat.) degrees in Computer Science with honors from TU Dortmund in 1992 and 1997. From 1997-2001 he was the Chief Engineer at the Embedded Systems Chair at TU Dortmund. In 2002, he joined RWTH Aachen University as a professor for Software for Systems on Silicon. His research comprises embedded software development tools, multicore processor architectures, hardware security, and system-level electronic design automation. He served in committees of the leading international EDA conferences and received various scientific awards, including Best Paper Awards at DAC and twice at DATE, as well as several industrial awards. Dr. Leupers is also engaged as an entrepreneur and in turning research results into innovations. He holds several patents and has been a co-founder of LISATek (now with Synopsys), Silexica, and Secure Elements. As the coordinator of the TETRACOM and TETRAMAX projects, he contributes to EU-wide academia-to-industry technology transfer.
Call for Papers (draft)

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:** July 30, 2021
- **Author notification:** September 25, 2021
- **Revised manuscript submission:** October 25, 2021
- **Final manuscript submission:** November 25, 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.