Call for Papers

Hardware Security in Emerging Technologies: Vulnerabilities, Attacks and Solutions

Guest editors:
- Naghmeh Karimi, University of Maryland Baltimore County, USA (Corresponding Guest Editor)
- Kanad Basu, University of Texas at Dallas, USA
- Chip-Hong Chang, Nanyang Technological University, Singapore
- Jason M. Fung, Intel Corporation, USA

Scope and Purpose

High complexity and cost of design and fabrication of integrated circuits have invoked the outsourcing of design and fabrication to different parties across the globe. Such globalization of integrated circuits (IC) design flow has jeopardized the security and trustworthiness of ICs and introduced new security vulnerabilities including, but not limited to, tampering the circuit to insert malicious circuitry in terms of hardware Trojans, IC counterfeiting, leaking sensitive data, IC cloning and overproduction, Intellectual Property (IP) piracy, and so on. Such security threats can impose a significant financial burden to industry and government sectors, and end-users, and can also threaten the security and privacy of these sectors.

The recent research on hardware security has mainly focused on digital circuits and their 2-D implementation. In practice, the security of emerging technologies such as spintronic devices, microfluidic biochips, and emerging memory technologies has received less attention. This special issue motivates the researchers to focus more on tackling these security threats. In addition, security and trustworthiness issues of analog circuits, mixed signals, and RF circuits, as well as 3-D ICs, will be promoted by this manuscript. On the other hand, with the broad range of applications of IoT devices in all domains including scientific, military, autonomous vehicles, and civil, their high versatility and major societal impact, comes the increased vulnerability to security attacks. Accordingly, this special issue aims at providing the targeted readers with the new advances and challenges in IoT Security.

In recent years, Artificial Intelligence (AI) has become an integral feature of most distributed computing architectures. Thereby, design of secure AI hardware accelerators has become a principal competition among high technology industry sectors. On the other hand, deploying machine learning schemes to protect integrated circuits against IC counterfeiting, Trojan infestation, data leakage, etc. has received the lion’s share of attention. Edge intelligence, where big data analytics meets edge computing, ushers
new threat horizon in the Artificial Intelligence of Things (AIoT) era. Accordingly, AI for security and Security of AI accelerators are two main topics encouraged by the Guest editors. Moreover, the guest editors opt to promote the publications on the security of the EDA tools deployed throughout the chip design and fabrication process.

In summary, this special issue seeks contributions encompassing the following broad scopes:

- **Security of Emerging Technologies**: In an attempt to obtain better performance and area/power overhead, researchers are investigating devices beyond traditional CMOS technologies. These include spintronic devices, nanomaterials, superconducting electronics, and 2-D materials. Accordingly, this special issue anticipates contributions incorporating both security issues pertaining to these devices and how these devices can be used to address CMOS-based security issues like IC camouflaging. The scope of this proposal extends to security issues related to analog, mixed-signal and RF integrated circuits, as well as digital microfluidic biochips. Moreover, this special issue seeks contributions related to the hardware design of cryptography primitives like post-quantum cryptography and homomorphic computing.

- **Security of Internet-of-things (IoT)**: We live in a world of IoT, where each and every aspect of our everyday lives are connected to the internet, and hence, are prone to compromise using malicious software or Malware. Accordingly, this special issue anticipates papers in the domain of IoT security, including low-powered edge devices, automotives, cyber-physical systems, and biomedical devices. The scope also includes contributions addressing privacy issues of these devices as well as privacy-preserving architecture for the same.

- **Machine Learning and Edge Intelligence Security**: Over the past decade, machine learning and deep learning have found their footprints in various aspects of the society, like self-driving automobiles, recommender systems, etc. Not surprisingly, security researchers have also started using machine learning for detecting security violations. Accordingly, this special issue anticipates papers that apply machine learning for improving hardware security. Since a lot of machine learning applications are now being accelerated on dedicated hardware, this scope encompasses papers focusing on attacks and countermeasures on hardware accelerators for artificial intelligence and machine learning and secure neuromorphic computing architecture.

- **EDA for Security**: Along with designers, EDA engineers are also developing novel techniques to counter the threats of hardware security. Accordingly, this special issue anticipates papers focusing on EDA tools designed to improve hardware security and/or trust assurance. This scope also encompasses EDA tools that can be used to improve the security of multi-tenant FPGA systems.

**Topics of interest**

The special issue focuses on recent security threats and vulnerabilities in the area of hardware and pinpoints to their related countermeasures. The focus will be mainly on the following topics:

- Security of emerging nanotechnologies
- Security of analog, mixed-signal and RF integrated circuits
- Security of biomedical devices
- Preserving security and trust in digital microfluidic biochips
- Security vulnerabilities of 3-D ICs and related countermeasures
- Secure neuromorphic computing
- Machine learning and analytics to improve security assurance and operation
- Secure hardware for AI and machine learning
- Security and Trust verification of IoT devices and cyber physical systems
- Security and Trust in autonomous vehicles
Efficient hardware implementation of post-quantum cryptography and homomorphic encryption
- Privacy preserving hardware design
- Breakthrough in automated tools and methodologies to significantly improve product security and/or effectiveness of security assurance effort
- Systematic mitigations to address common security concerns in SoC design
- In-field security enhancement of deployed products
- Addressing security threats in multi-tenant FPGAs

Submission procedure
Prospective authors are invited to submit their papers following the instructions provided on the JETCAS website: https://mc.manuscriptcentral.com/jetcas. The submitted manuscripts should not have been previously published nor should they be currently under consideration for publication elsewhere.

Important dates
- Manuscript submissions due: 2020-12-07
- First round of reviews completed: 2021-01-31
- Notification to authors: 2021-02-10
- Revised manuscripts due: 2021-03-15
- Second round of reviews completed: 2021-04-15
- Notifications to authors: 2021-04-30
- Final manuscripts due: 2021-05-10
- Target publication date: 2021-06-30

Request for information
- Naghmeh Karimi (nkarimi@umbc.edu)