IGSC 2019 Workshop Proposal

Secure Analog Mixed-Signal Integrated Circuits: Challenges and Solutions

Format suggested: Six 45 minute presentations with a total time of approximately 5 hours.

Topics addressed

- Security challenges of analog and RF circuits
- Potential methods to secure AMS circuits
- Analog side-channels as information
- Machine learning methods to secure analog/RF ICs

Keywords: heterogeneous integration, power efficient circuits and systems.

Target audience and requisite knowledge of audience

The session theme is selected per the general theme of the conference. Our target audience is all attendees of the conference. Prior knowledge of hardware security or analog design, although not a requisite, provides a sound basis of the topics presented by the speakers.

Workshop overview

Despite economic benefits, the globalization of the design and manufacturing of integrated circuits has led to increased vulnerabilities in multiple aspects of system integrity. During the design of a circuit, intellectual property (IP) piracy and tampering with circuit specifications to modify the intended functionality pose risks to the system. Outsourcing fabrication provides opportunities for untrusted parties to tamper, overproduce, and clone an IC. Even after the release of an IC to market, the circuit structure is vulnerable to non-invasive reverse engineering (RE). In addition, although significant effort and progress has been made in the security of digital circuits, techniques and methodologies to secure analog and RF circuits lag behind. The general topic covered in this workshop is, therefore, an analysis of threat challenges in the analog and mixed-signal IC domain as well as an overview of early techniques to protect such circuits from nefarious acts. The goal is for participates to better understand the security challenges of analog/RF mixed signal circuits including particular vulnerabilities, means of exploitation, and methods to secure these ICs from potential adversaries.

Workshop Organizer: Ioannis Savidis (Drexel University)

Biography: Ioannis Savidis received the B.S.E. degree in electrical and computer engineering and biomedical engineering from Duke University, Durham, NC, in 2005. He received the M.Sc. and Ph.D. degrees in electrical and computer engineering from the University of Rochester, Rochester, NY, USA, in 2007 and 2013, respectively.

He is an Associate Professor with the Department of Electrical and Computer Engineering at Drexel University, Philadelphia, PA, USA, where he directs the Integrated Circuits and Electronics (ICE) Design and Analysis Laboratory. His current research and teaching interests include analysis, modeling, and design methodologies for high performance digital and mixed-signal integrated circuits, power management for SoC and microprocessor circuits (including on-chip dc-dc converters), hardware security (logic obfuscation), and interconnect related issues, with a specific emphasis on electrical and thermal modeling and characterization, signal and power integrity, and power and clock delivery for heterogeneous 2-D and 3- D circuits.

Dr. Savidis is a recipient of the 2018 National Science Foundation Early Faculty (CAREER) Award. He serves on the organizing committees of the IEEE International Symposium on Hardware Oriented Security and Trust, the ACM Great Lakes Symposium on VLSI, and the International Verification and Security Workshop. He is a member of the Association of Computing Machinery, IEEE Circuits and Systems Society, IEEE Communications Society, and the IEEE Electron Devices Society. He also serves on the editorial boards of the *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, the *Microelectronics Journal*, and the *Journal of Circuits, Systems and Computers*.