IEEE CS Student Chapter Presents

Analog Circuit Security in the Digital World

Dr. Yier Jin

Endowed Term Professor, Associate Professor
Department of Electrical and Computer Engineering,
University of Florida, Gainesville

3:30 PM, ENB 228
Friday, 2nd November 2018

The rapid growth and globalization of the integrated circuit (IC) industry put the threat of hardware Trojans (HTs) front and center among all security concerns in the IC supply chain. Current Trojan detection approaches always assume HTs are composed of digital circuits. However, recent demonstrations of analog attacks, such as A2 and Rowhammer, invalidate the digital assumption in previous HT detection or testing methods. At the system level, attackers can utilize the analog properties of the underlying circuits such as charge-sharing and capacitive coupling effects to create information leakage paths. To address these stealthy yet harmful threats, we identify a large class of such capacitor-enabled attacks and define them as charge-domain Trojans. We are able to abstract the detailed charge-domain models for these Trojans and expose the circuit-level properties that critically contribute to their information leakage paths. The proposed method is validated on an experimental RISC microcontroller design injected with different variants of charge-domain Trojans. We demonstrate that successful detection can be accomplished with an automatic toolset.

is the Endowed IoT Term Professor in the Warren B. Nelms Institute for the Connected World and also an Associate Professor in the Department of Electrical and Computer Engineering (ECE) in the University of Florida (UF). Prior to joining UF, he was an assistant professor in the ECE Department at the University of Central Florida (UCF). He received his PhD degree in Electrical Engineering in 2012 from Yale University after he got the B.S. and M.S. degrees in Electrical Engineering from Zhejiang University, China, in 2005 and 2007, respectively. His research focuses on the areas of embedded systems design and security, trusted hardware intellectual property (IP) cores and hardware-software co-design for modern computing systems. His is currently focusing on the design and security analysis on Internet of Things (IoT) and wearable devices with particular em