IC Level Trojan Detection

ECE Group 46

Abstract

An Integrated Circuit (IC) is an electronic circuit formed on a small piece of semiconducting material, used to implement a multitude of computational and sensory tasks. ICs implement memory, timers, amplifiers, microprocessors, and many other functions. ICs are integrated to build everyday devices such as a Bluetooth headset, remote, or a router. Companies outsource IC fabrication to reduce the cost of manufacturing, as modern fabrication costs are in the billions. The design of an IC is therefore easily accessed by outside entities which leads to the IC being potentially compromised by the insertion of a Trojan, a malicious modification or insertion of undesired functionality of an IC. The Trojan compromises the IC by modifying the functionality, the specifications, or by simply leaking data. Trojans are injected at different levels of the design and fabrication process such as through untrusted foundries, third party IPs, synthesis tools and libraries, testing and verification tools, and configuration scripts. The infected IC becomes a security risk for the manufacturer and a privacy risk for consumers. While there are methods to detect Trojans within the workflow, there is no method for real-time detection, allowing Trojans to go undetected. We are developing a Hardware Trojan Detection technique by using an algorithm that can detect, in real-time, a Trojan on an IC. By implementing side-channel analysis of the noise on the power rails, an understanding of the noise patterns exhibited on the IC, a baseline for power analysis can be created for the algorithm. From the power profile of the IC, modification to the IC will lead to detectable changes to the noise profile of the power network