On-Chip Real-Time Hardware Trojan Detection

Ioannis Savidis (PI)

Challenge:

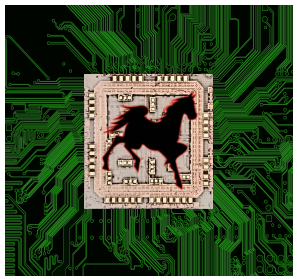
Untrusted third parties are found throughout the integrated circuit supply chain and can modify the intended design of an integrated circuit

Determining modifications to the design of an IC requires novel circuit techniques and methodologies

Solution:

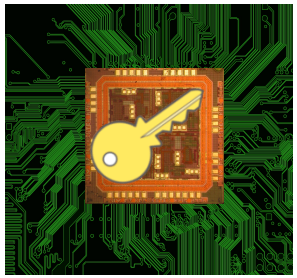
Monitor noise on the on-chip power network to determine the presence of hardware Trojans:

- On-chip distributed sensory network for Trojan detection
- Adversarial dynamics for placement heuristics of sensors
- Post-detection recovery from a Trojan through a discretized power delivery network



Current solutions: Post-fabrication testing of a modified circuit limited to activation of a T n

Our solution: Improved integrated circuit security through run-time on-chip side-channel monitoring



Scientific Impact:

- Novel detection methodologies that enhance identification and localization of Trojans in real-time
- Circuit countermeasures that allow for continued use of an IC post-detection of Trojan
- Algorithms to integrate security into the IC design flow

Broader Impact:

Securing electronic assets by assuring the integrated circuits that are installed do not include modified functions

Outreach via:

- Program that pairs sophomores and juniors at local high schools with Drexel faculty mentors
- Curriculum development for a new course in Hardware Security as part of the M.S. degree in Cybersecurity

PIs: Ioannis Savidis (Drexel University)
Contact: isavidis@coe.drexel.edu, 215-571-4584
Webpage: http://ice.ece.drexel.edu