Techniques for Creation and Insertion of Test Points for Malicious Circuitry Detection

Tech ID: 30202 / UC Case 2012-745-0

SUMMARY

Researchers led by Dr. Potkonjak from the UCLA Department of Computer Science have developed a technique to detect hardware Trojans in integrated circuits.

BACKGROUND

Integrated circuits (ICs) play key roles in most of today's technologies ranging from mobile devices to computers. The high cost of fabricating ICs results in the dominance of a contract-foundry semiconductor business model in which multiple independent entities come together to create large batches of ICs to defray the cost. This process leaves ICs vulnerable to hardware Trojans, unwanted components added to ICs during the manufacturing process that enable monitoring or spying. Trojans are currently detected using side channel measurements of delay and power leakage. However, inherent variation in the production of ICs along with the complexity of their circuits allows Trojans to hide in ICs undetected.

INNOVATION

Researchers led by Dr. Potkonjak from the UCLA Department of Computer Science have developed a technique to detect hardware Trojans in integrated circuits. The effectiveness of current Trojan detection decreases with complex circuit paths with many convergence points and with Trojans that look like inherent IC variation. Their invention uses a set of test points that can detect hardware Trojans regardless of the convergence of IC paths and inherent variation. This invention can be applied to any arbitrary IC design to provide robust and effective Trojan detection. Furthermore, this invention uses very little computational overhead (<5%).

APPLICATIONS

- Hardware Trojan detection
- Maintenance of ICs
- Calculating life expectancy of ICs

ADVANTAGES

- Flexible to any IC design
- Inexpensive
- Low computational overhead
- Robust

CONTACT

UCLA Technology Development Group
ncd@tdg.ucla.edu
tel: 310.794.0558.

INVENTORS

- Potkonjak, Miodrag

OTHER INFORMATION

KEYWORDS

Integrated circuits, FPGA, computer, hardware, fabrication, power leakage, delay measurements, Trojan, malware

CATEGORIZED AS

- **Computer**
  - Hardware
  - Security
- **Security and Defense**
  - Other
- **Semiconductors**
  - Design and Fabrication
  - Other
  - Testing

RELATED CASES

2012-745-0

UCLA Technology Development Group
10889 Wilshire Blvd., Suite 920,Los Angeles,CA 90095
tdg.ucla.edu
Tel: 310.794.0558 | Fax: 310.794.0638 | ncd@tdg.ucla.edu