EL 9453: Introduction to Hardware Security and Trust

Syllabus

Instructor: Prof. Ramesh Karri (rkarri@nyu.edu; cell: 917 363 9703)

Pre-requisites: EL 5493/EL4313 and/or EL 5473/EL3913 and/or Computer Architecture and/or Real Time Embedded Systems Design

Motivation: Globalization has led to outsourcing of design, fabrication, test and packaging of ICs. Rogue elements in any of these phases can alter the design and embed malicious circuits. These malicious circuits may be triggered some time in the future. Classical VLSI design and test methods are inadequate to detect these malicious circuits. Even if there are no malicious circuits in designs, side channels of an implementation can leak the secrets and intellectual property. Examples include power, timing, EM radiation and deliberately introduced faults. Finally, the testing infrastructure used to improve the quality of ICs can be used to leak secrets.

Objective: Students will be introduced toall aspects of a VLSI design. The students will be exposed to defenses that can detect and protect against the variety of discussed threats. Following is a tentative list of topics that will be covered in the course:

Topic	Weeks
Introduction; Homework 1 on example hardware attacks not covered in class	1
Ciphers: Historical; Block (AES/DES), stream, (Trivium) public key ciphers (RSA. ECC), hash functions (SHA-1); Homework on the various ciphers	2
Physical unclonable functions: design principles and applications; Hardware Random Number Generators: design principles and applications; Lab: Design and Evaluate PUFs and Random Number Generators on an FPGA	2
Side channels: Overview; Fault attacks and countermeasures; Power attacks and countermeasures; Lab: Design a fault attack and evaluate a countermeasure	2
VLSI Testing is a portal for hackers: attacks and countermeasures; Lab: scan attack on FPGA implementation of DES	2
Hardware Trojans: overview, attacks and defenses; Lab: Malicious 8051 processor design	1
IP Piracy: Logic encryption; Lab: FPGA logic encryption of combinational logic	1
Reverse Engineering: IC layout camouflaging, Gate level reversing, ESL reversing	2

Hardware security patent presentations	1
Final exam	1

Present a patent on a topic: present patents or research papers

Course Project:(six-weeks). Deliverables: a six-page conference style report. Example projects include malicious processor design, reverse engineering ESL, security validation, fault and test attacks on block and stream ciphers, countermeasures etc., IC Camouflaging, aging attacks etc…

Course material: Papers from IEEE journals (Transactions on CAD, Computers, Information forensics and Security and VLSI), Proceedings of 2008-2013 IEEE workshops on Hardware Oriented Security and Trust (HOST), Proceedings of Workshop on Cryptographic Hardware and Embedded Systems; NYU-Poly Embedded Systems Challenge reports. Please use IEEE explore for the papers from IEEE journals.

Grading: Assignments/Labs: 30%, patent presentation: 15%; project 45% final exam: 10%