Course Overview: EE4773/5773 Foundations of Hardware Security

Description

This course explores the basic concepts of hardware security, distinguishing it from software, network, and system security. Through lab sessions, students gain hands-on experience in performing attacks, developing countermeasures, and implementing secure hardware building blocks. The course encourages students to engage with contemporary issues and recent research in the field of hardware security. Students are expected to have foundational knowledge of digital logic and Register-Transfer Level (RTL) design, though no specific background in security or cryptography is required.

Course Objective

The course aims to equip students with a comprehensive understanding of hardware security principles, preparing them to address modern challenges and contribute to advancements in the field.

Requisite: EE 3954

Instructor: Ahmed Oun

Schedule

- **Days:** Tuesday and Thursday
- **Time:** 11:00 am – 12:20 pm
- **Location:** ARC 312 (except during lab sessions)

Key Course Topics

1. Introduction & background on hardware design
2. Ethics and Attacks Overview, Countermeasures and Security Primitives
3. Board Level Reverse Engineering & Countermeasures
4. Integrated Circuit Reverse Engineering& Countermeasures
5. Reverse Engineering cont., KiCad Introduction and Demo
6. Hardware Trojans and 3rd party IP, Verilog Basics and FPGAs
7. Side Channel Attacks
8. Hardware Security Primitives: PUFs, TRNGs, Hardware obfuscation
9. Contemporary issues and recent research