EEE4346C

HARDWARE SECURITY & TRUSTED CIRCUIT DESIGN

OVERVIEW OF THIS COURSE

The purpose of this course is to introduce a newly emerged area, trusted integratedcircuits and prepare students for challenges in the field of hardware security. The concept andtaxonomy of hardware Trojans will be introduced as well as their malicious impact to both critical and commercial device. Considering the fact that cryptographic embedded systems are often the target of hardware Trojans, cryptographic embedded systems and their vulnerabilities when attacked by hardware Trojans will also be discussed in the course

The course will also prepare students for the Embedded System Challenge in Cybersecurity Awareness Week (CSAW) hosted by NYU-Poly every November. Therefore, the objective of the course are (1) to give students the idea of hardware security: identify the vulnerabilities of circuit designs, (2) to understand the principles of hardware Trojan detection methods and propose new detection methods to ensure the trustworthiness of the integrated circuits, and (3) to prepare students for the challenge of embedded system security. Proposed circuit trust evaluation methods will be simulated based on commercial EDA tools.

LECTURE TOPICS

- Introduction to hardware security
- Introduction to cryptographic embedded systems
- Security issues in processors and microprocessors
- A review of hardware Trojan detection methods
- Fault attacks and countermeasures
- Design of Physical Unclonable Function (PUF)
- Advanced topics in hardware security

COURSE INSTRUCTOR
DR. YIER JIN
DEPARTMENT OF EECS
UNIVERSITY OF CENTRAL FLORIDA

UCF College of Engineering and Computer Science