University of California Davis

Introduction to Hardware Security
Syllabus
Winter 2022

Course Objectives
This course will cover topics related to hardware security including: Cryptographic processing and the analysis of its overhead, physical attacks, side-channel attacks and counter measures, physically unclonable functions, hardware-based random number generators, watermarking of Intellectual Property (IP) blocks, FPGA security, PCB security, passive and active metering for prevention of piracy, and access control. Background on digital design is neded. Introductory lectures will cover basic background on cryptography, authentication, secret sharing, and VLSI design. The main goals for this course are:

· Learning the state-of-the-art security methods and primitives
· Integration of security as a design metric, not as an afterthought
· Better understanding of attacks and providing countermeasures against them
· hands-on learning approach, via projects, homework's, and review assignments

ECE 289Q Part 1 (Introduction to Hardware Security) offering is in person. The lectures will be uploaded on weekly basis. Each lecture is 1.5 hours in length.

Course Outline

Week	Lecture
1	Course Syllabus, Ethics, and Introduction to Cryptography
2	Basics of VLSI Design and Test
3	Security Based on PUFs and TRNGs
4	Hardware Metering
6	Watermarking of HW Ips + Student Presentation
7	**Midterm Exam**
8	Physical Attacks and Fault Injection Attacks + Student Presentation
9	PCB Security + Student Presentation
10	Side Channel Attacks and Countermeasures + Student Presentation

Class Meetings

According to the literature cited in the Association for the Study of Higher Education (ASHE) report, in order for students to learn they must do more than just listen: they must read, write, discuss, or be engaged in solving problems. In particular, students must engage in such higher-order thinking tasks as analysis, synthesis, and evaluation. Active learning engages students in two aspects – doing things and thinking about the things they are doing. [Wikipedia: Active Learning]

Active learning is the process whereby students engage in activities, such as reading, writing, discussion, or problem solving, that promote analysis, synthesis, and evaluation of class content. [University of Michigan – Center for Research on Learning and Teaching. http://www.crlt.umich.edu/tstrategies/tsal]

Format: The course is comprised of weekly lectures, 4 HW assignments, student paper presentations, and a final project. In addition, there will be two exams (midterm + final).

Prerequisites:

EEC 18 or EEC 118, or equivalent

Textbooks:
S. Bhunia and M. Tehranipoor, Hardware Security: A Hand-on Training Approach, Morgan Kauffman, 2018
Reference Book:
M. Tehranipoor and C. Wang (Eds.), Introduction to Hardware Security and Trust, Springer, 2011

Exams

This course includes one Midterms exams and a Final exam. Exam dates are specified in the course schedule. Each exam will consist of: (1) a set of multiple-choice questions; and (2) several long-answer questions.

All exams are cumulative. All exams are closed book.

Course Grade

The exams, assignments, projects and class problems will be used to determine your final grade according to the following weighting:

Assignments and Projects	40%
Presentation	10%
Midterm Exam	20%
Final Exam	30%