Introduction to Hardware Security and Trust
EEE4714/EEE5716

Class Periods: Tuesday (08-09) and Thursday (09)
Academic Term: Spring 2020
Location: NEB 201
Instructor: Mark Tehranipoor

Instructor/coordinator:	**Dr. Mark Tehranipoor**
Office Location	MAE 226
Office Hours	Mon 2-3pm
Class Location	NEB 201
Telephone	352-392-2585
Email	tehranipoor@ece.ufl.edu
Website	http://tehranipoor.ece.ufl.edu

Catalog Description

Fundamentals of hardware security and trust for integrated circuits and systems, cryptographic hardware, invasive and non-invasive attacks, side-channel attacks, physically unclonable functions (PUFs), true random number generation (TRNG), watermarking of Intellectual Property (IP) blocks, FPGA security, counterfeit ICs, hardware Trojans in IP cores and ICs. Lecture. Credits 3.

Pre-requisites

EEE3701C: Digital Logic (or equivalent)

Course Objectives

This course will cover the following topics: Cryptographic processor and processing overhead analysis, physical and invasive attacks, side-channel attacks, physically unclonable functions, hardware-based true random number generators, watermarking of Intellectual Property (IP) blocks, FPGA security, passive and active metering for prevention of piracy, access control, hardware Trojan detection and isolation in IP cores and integrated circuits (ICs). The course is largely self-contained. Background on digital design would be sufficient. Introductory lectures will cover basic background on cryptography, authentication, secret sharing, VLSI design, test and verification. 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
- A hands-on learning approach, via projects, homeworks, and review assignments

Supervised Teaching Assistants (STAs)

Jason Vosatka, jvosatka@ufl.edu	(Wed 3-4pm)
Nitin Pundir, nitin.pundir@ufl.edu	(Wed 3-4pm)
Dhwani Mehta, dhwanimehta@ufl.edu	(Wed 3-4pm)
Nusrat Farzana, ndipu@ufl.edu	(Wed 3-4pm)

The STAs will lead about half of the Thursday lectures and will assist with evaluation of student modules and final projects.

Meeting Times

Days	Period	Time
Tuesday	08-09	3:00-4:55PM
Thursday	09	4:05-4:55PM

When the instructor is on travel, pre-recorded lectures will be made available on Canvas well before the class. Students are expected to view the lectures, come to the class, and take quiz. After the quiz is done, STAs will be available to answer any questions and concerns you may have about the lecture.

Meeting Location (for In-campus students) - NEB 201

Material and Supply Fees

Avnet Spartan-6 LX9 MicroBoard (or equivalent FPGA boards) for each project team ($~100/team) – each team may include up to 3 students. (https://www.xilinx.com/products/boards-and-kits/1-3i2dfk.html)

Textbooks and Software Required

Textbook:

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

Software: Xilinx ISE package, Synopsys Verilog simulation package and HSpice, Cadence Design System, Programming and Scripting Software (Matlab, Python, C/C++)

Recommended Reading and Videos

Reading

- Mihir Bellare and Phil Rogaway, Introduction to Modern Cryptography
- Ross J. Anderson. Security Engineering: A guide to building dependable distributed systems. John Wiley and Sons, 2001
- Matt Bishop , Computer Security: Art and Science, Addison-Wesley, 2003
- William Stallings. Cryptography and Network Security, Fourth edition, 2007
- The Hunt for the Kill Switch
- Hardware Trojan (computing)
- Defense Science Board Task Force On High Performance Microchip Supply
- Old Trick Threatens the Newest Weapons
- A Survey of Hardware Trojan taxonomy and Detection
- Detecting malicious inclusions in secure hardware: Challenges and Solutions
- FPGA Design Security Bibliography
- Supergeek pulls off 'near impossible' crypto chip hack
- Security through obscurity
- Trust-Hub

Videos

- What's inside a microchip? http://www.youtube.com/watch?v=GdqbLmdKgw4
- Zoom Into a Microchip http://www.youtube.com/watch?v=Fxv3JoS1uY8
- Public Key Cryptography: RSA Encryption: http://www.youtube.com/watch?v=wXB-V_Keiu8

- Counterfeit Electronics Could Be Dangerous, Funding Nefarious People http://www.youtube.com/watch?v=dbZiUe6guxc
- How Computers and Electronics Are Recycled http://www.youtube.com/watch?v=Iw4g6H7alvo
- Counterfeit Electronic Components Process http://www.youtube.com/watch?v=5vN_7NJ4qYA
- Counterfeit Inspection http://www.youtube.com/watch?v=MbQUvu2LN6o
- Gold from waste circuit electronics http://www.youtube.com/watch?v=ZkhOuNvkuu8
- Tarnovsky Deconstruct Processor https://www.youtube.com/watch?v=w7PT0nrK2BE
- AES cipher visualization (link https://www.youtube.com/watch?v=mlzxpkdXP58)

Course Outline

Week	Tuesday Lecture	Instructor	Thursday Lecture	Instructor
Week 1 (Jan 7, 9)	Syllabus, Ethics, Introduction to hardware security and trust, Emerging applications and the new threats	MT	Cont. Introduction to hardware security	MT
Week 2 (Jan 14, 16)	Introduction to Cryptography	MT	Introducing Tuesday Activities + VHDL/Verilog & FPGA Tutorial	STA
Week 3 (Jan 21, 23)	Basics of VLSI Design and Test	MT	VHDL/Verilog & FPGA Tutorial	STA
Week 4 (Jan 28, 30)	Security Based on PUFs and TRNGs	MT	VHDL/Verilog & FPGA Tutorial	STA
Week 5 (Feb 4, 6)	Hardware Metering	MT	CAD Tools	STA
Week 6 (Feb 11, 13)	Watermarking of HW IPs	MT	Project Description	MT/ STA
Week 7 (Feb 18, 20)	Physical Attacks and Fault Injection Attacks	MT	Student Presentations	MT/ STA
Week 8 (Feb 25, 27)	**Midterm**	MT	Student Presentations	MT/ STA
Week 9	SPRING BREAK			
Week 10 (Mar 10, 12)	Hardware Trojans: IC Trust (Taxonomy and Detection)	MT	Student Presentations	MT/ STA
Week 11 (Mar 17, 19)	Hardware Trojans: IP Trust (Detection) + Design for Hardware Trust	MT	Student Presentations	MT/ STA
Week 12 (Mar 24, 26)	Counterfeit Detection and Avoidance	MT	Student Presentations	MT/ STA
Week 13 (Mar 31, Apr 2)	Basics of PCB Security + FGPA Security	MT	Student Presentations	MT/ STA
Week 14 (Apr 7, 9)	Protecting against Scan-based Side Channel Attacks	MT	Student Presentations	MT/ STA
Week 15 (Apr 14, 16)	Side Channel Attacks and Countermeasures, Countermeasures for Embedded Microcontrollers	MT	Student Presentations	MT/ STA
Week 16 (Apr 21)	Final Class – Review Final Exam	MT		
April 28	**12:30-2:30pm, Room NEB 201**			
May 4	**Grades due**			

Attendance and Expectations

Format: The course is comprised of weekly lectures, 3-4 HW assignments, student paper presentation module, and a final project. In addition, there will be two exams (midterm + final) and surprise pop quizzes.

Students must submit ***individual*** work ***individually*** on each module and as a team of 3 on final project. You are encouraged to work together on homework assignments and share ideas on lab assignments. However, you are not allowed to copy or duplicate any lab material (code, drawings, etc.) from another student. It will be considered cheating and will be dealt with in a severe manner. See Section 16 on Honesty Policy.

The final project will require implementation of a hardware security primitive or attack on an FGPA based on several conference and journal papers distributed to the teams. The team's work will be evaluated through demonstration on several benchmarks. Each group will prepare a presentation, demonstration of the project, and final report. The final report will discuss challenges met, present in-depth analysis of the approaches implemented by the team, etc.

The EDGE students may complete the paper presentation and final project module individually or as a team of 3. A separate instruction set will be issued for individual paper presentations and projects.

Grading-methods of evaluation

- Exams 40% (20% mid-term, 20% final (comprehensive, more emphasis on post-mideterm topics))
- HW Assignments 15%
- Final Project 20%
- Oral Paper Presentation 15%
- Quiz 10%

Grading Scale

Grading scale for the course: ≥90 A, ≥87 A-, ≥80 B, ≥77 B-, ≥ 70 C,≥ 67 C-,≥ 60 D, ≥ 57 D-,<57 F

Make-up Exam Policy

For the pass/fail evaluation of each module, students are allowed two tardy passes where a tardy is any module checked-off after the initial scheduled time. The tardy extension can be up to one week only and if a student falls too far behind they will be strongly encouraged to drop the class. After the first two free tardy extensions are used, additional tardy extensions result in a partial grade penalty – i.e. A=>A-…C-=>D+, one grade lower automatically per unsanctioned tardy.

Accommodation for Students with Disabilities

Students requesting classroom accommodation must first register with the Dean of Students Office. That office will provide the student with documentation that he/she must provide to the course instructor when requesting accommodation.

UF Counseling Services

Resources are available on-campus for students having personal problems or lacking clear career and academic goals. The resources include:
University Counseling Center, 301 Peabody Hall, 392-1575, Personal and Career Counseling.

SHCC mental Health, Student Health Care Center, 392-1171, Personal and Counseling.
Center for Sexual Assault/Abuse Recovery and Education (CARE), Student Health Care Center, 392-1161, sexual assault counseling.
Career Resource Center, Reitz Union, 392-1601, career development assistance and counseling.

Students Requiring Accommodations

Students with disabilities requesting accommodations should first register with the Disability Resource Center (352-392-8565, https://www.dso.ufl.edu/drc) by providing appropriate documentation. Once registered, students will receive an accommodation letter which must be presented to the instructor when requesting accommodation. Students with disabilities should follow this procedure as early as possible in the semester.

Course Evaluation

Students are expected to provide professional and respectful feedback on the quality of instruction in this course by completing course evaluations online via GatorEvals. Guidance on how to give feedback in a professional and respectful manner is available at https://gatorevals.aa.ufl.edu/students/. Students will be notified when the evaluation period opens, and can complete evaluations through the email they receive from GatorEvals, in their Canvas course menu under GatorEvals, or via https://ufl.bluera.com/ufl/. Summaries of course evaluation results are available to students at https://gatorevals.aa.ufl.edu/public-results/.

University Honesty Policy

UF students are bound by The Honor Pledge which states, "We, the members of the University of Florida community, pledge to hold ourselves and our peers to the highest standards of honor and integrity by abiding by the Honor Code. On all work submitted for credit by students at the University of Florida, the following pledge is either required or implied: "On my honor, I have neither given nor received unauthorized aid in doing this assignment." The Honor Code (https://sccr.dso.ufl.edu/policies/student-honor-code-student-conduct-code/) specifies a number of behaviors that are in violation of this code and the possible sanctions. Furthermore, you are obligated to report any condition that facilitates academic misconduct to appropriate personnel. If you have any questions or concerns, please consult with the instructor or TAs in this class.

Commitment to a Safe and Inclusive Learning Environment

The Herbert Wertheim College of Engineering values broad diversity within our community and is committed to individual and group empowerment, inclusion, and the elimination of discrimination. It is expected that every person in this class will treat one another with dignity and respect regardless of gender, sexuality, disability, age, socioeconomic status, ethnicity, race, and culture.

If you feel like your performance in class is being impacted by discrimination or harassment of any kind, please contact your instructor or any of the following:

- Your academic advisor or Graduate Program Coordinator
- Robin Bielling, Director of Human Resources, 352-392-0903, rbielling@eng.ufl.edu
- Curtis Taylor, Associate Dean of Student Affairs, 352-392-2177, taylor@eng.ufl.edu
- Toshikazu Nishida, Associate Dean of Academic Affairs, 352-392-0943, nishida@eng.ufl.edu

Software Use

All faculty, staff, and students of the University are required and expected to obey the laws and legal agreements governing software use. Failure to do so can lead to monetary damages and/or criminal penalties for the individual violator. Because such violations are also against University policies and rules, disciplinary action

will be taken as appropriate. We, the members of the University of Florida community, pledge to uphold ourselves and our peers to the highest standards of honesty and integrity.

Student Privacy

There are federal laws protecting your privacy with regards to grades earned in courses and on individual assignments. For more information, please see: https://registrar.ufl.edu/ferpa.html