Introduction to Hardware Security and Trust
EEE4714/EEE5716

Class Periods: Tuesday (08-09) and Thursday (09)
Academic Term: Spring 2021
Location: NEB 201
Instructor: Farimah Farahmandi

Instructor/coordinator: **Dr. Farimah Farahmandi**
(Some lectures will be given by Dr. Tehranipoor)

Office Location	Virtual/Zoom
Office Hours	Tuesday 4-5pm
Class Location	NEB 201
Telephone	Email Only
Email	ffarahmandi@ufl.edu
Website	http://farimah.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

EEL 3701: Digital Logic and Computer Systems

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, homework, and review assignments

Supervised Teaching Assistants (STAs)

Tao Zhang, tao.zhang@ufl.edu	(Wed 3-4pm)
Nurun Mondol, nmondol@ufl.edu	(Wed 3-4pm)
Kawser Bepary, mdkawser.bepary@ufl.edu	(Wed 3-4pm)
Jacob Harrison, jacob.harrison@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 (Fall 2022 class is held 100% in person, Tuesday (08-09) and Thursday (09))

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

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 (Aug 22)			Syllabus, Ethics, Introduction to hardware security and trust,	MT
Week 2	Syllabus, Ethics, Introduction to hardware security and trust, Emerging applications and the new threats	MT	Cont. Introduction to hardware security	MT
Week 3	Introduction to Cryptography	FF	Introducing Tuesday Activities + VHDL/Verilog & FPGA Tutorial	STA
Week 4	Basics of VLSI Design and Test	FF	VHDL/Verilog & FPGA Tutorial	STA
Week 5	Security Based on PUFs and TRNGs	FF	Project Description	STA
Week 6	Hardware Metering	FF	VHDL/Verilog & FPGA Tutorial	STA
Week 7	Watermarking of HW IPs	FF	CAD Tools	MT/ STA
Week 8	Physical Attacks and Fault Injection Attacks	FF	Student Presentations (Students should record their presentation and share to be viewed by others prior to assigned dates)	FF/ STA
Week 9	**Midterm**	FF	Student Presentations	FF/ STA
Week 10	Hardware Trojans: IC Trust (Taxonomy and Detection)	FF	Student Presentations	FF/ STA
Week 11	Hardware Trojans: IP Trust (Detection) + Design for Hardware Trust	FF	Student Presentations	FF/ STA
Week 12	Counterfeit Detection and Avoidance	FF	Student Presentations	FF/ STA
Week 13	Basics of PCB Security + FGPA Security	FF	Student Presentations	FF/ STA
Week 14	Protecting against Scan-based Side Channel Attacks	FF	Student Presentations	FF/ STA
Week 15	Side Channel Attacks and Countermeasures, Countermeasures for Embedded Microcontrollers	FF	Student Presentations	FF/ STA
Week 16 (Dec 7)	Final Class – Review Final Exam	FF		
Final Exam	12/15/2022 @ 3:00 PM - 5:00 PM			
Dec 19	**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

Late submission

Late assignment submissions will not be accepted unless prior arrangements have been made between the student and TA/Professor.

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

Health and Wellness

Covid-19 Protocols:

- You are expected to wear approved face coverings at all times during class and within buildings even if you are vaccinated. Please continue to follow healthy habits, including best practices like frequent hand washing. Following these practices is our responsibility as Gators.

- If you are sick, stay home and self-quarantine. Please visit the UF Health Screen, Test & Protect website about next steps, retake the questionnaire and schedule your test for no sooner than 24 hours after your symptoms began. Please call your primary care provider if you are ill and need immediate care or the UF Student Health Care Center at 352-392-1161 (or email covid@shcc.ufl.edu) to be evaluated for testing and to receive further instructions about returning to campus. UF Health Screen, Test & Protect offers guidance when you are sick, have been exposed to someone who has tested positive or have tested positive yourself. Visit the UF Health Screen, Test & Protect website for more information.

U Matter, We Care:
Your well-being is important to the University of Florida. The U Matter, We Care initiative is committed to creating a culture of care on our campus by encouraging members of our community to look out for one another and to reach out for help if a member of our community is in need. If you or a friend is in distress, please contact umatter@ufl.edu so that the U Matter, We Care Team can reach out to the student in distress. A nighttime and weekend crisis counselor is available by phone at 352-392-1575. The U Matter, We Care Team can help connect students to the many other helping resources available including, but not limited to, Victim Advocates, Housing staff, and the Counseling and Wellness Center. Please remember that asking for help is a sign of strength. In case of emergency, call 9-1-1.

Counseling and Wellness Center: https://counseling.ufl.edu, and 392-1575; and the University Police Department: 392-1111 or 9-1-1 for emergencies.

Sexual Discrimination, Harassment, Assault, or Violence
If you or a friend has been subjected to sexual discrimination, sexual harassment, sexual assault, or violence contact the **Office of Title IX Compliance**, located at Yon Hall Room 427, 1908 Stadium Road, (352) 273-1094, title-ix@ufl.edu

Sexual Assault Recovery Services (SARS)
Student Health Care Center, 392-1161.

University Police Department at 392-1111 (or 9-1-1 for emergencies), or http://www.police.ufl.edu/.

Academic Resources

E-learning technical suppor*t*, 352-392-4357 (select option 2) or e-mail to Learning-support@ufl.edu. https://lss.at.ufl.edu/help.shtml.

Career Resource Center, Reitz Union, 392-1601. Career assistance and counseling; https://career.ufl.edu.

Library Support, http://cms.uflib.ufl.edu/ask. Various ways to receive assistance with respect to using the libraries or finding resources.

Teaching Center, Broward Hall, 392-2010 or 392-6420. General study skills and tutoring. https://teachingcenter.ufl.edu/.

Writing Studio, 302 Tigert Hall, 846-1138. Help brainstorming, formatting, and writing papers. https://writing.ufl.edu/writing-studio/.

Student Complaints Campus*:* https://sccr.dso.ufl.edu/policies/student-honor-code-student-conduct-code/;https://care.dso.ufl.edu.

On-Line Students Complaints*:* http://www.distance.ufl.edu/student-complaint-process.