Advanced Hardware Security and Trust
EEE 6742
Class Periods: T, 10, 5:10PM-6:00PM; R, 10-11, 5:10PM-7:05PM
Location: MAEB 0211
Academic Term: Fall 2022

Instructor:

Name:	Dr. Domenic Forte
Email:	dforte@ece.ufl.edu
Telephone:	352-392-1525
Office Hours:	Tuesdays, 9AM-11AM (Zoom – link shared on Canvas)

Teaching Assistant/Peer Mentor/Supervised Teaching Student:
Please contact through the Canvas website

- TBD

Course Description
This course expands on the foundation provided by the Introduction to Hardware Security and highlights the challenges arising from the end of Moore's law as well as the rapid evolution of attackers. Hands-on experience with various commercial and open-source CAD tools will be developed via lectures, tutorials, and projects. *Lecture. Credits 3.*

Course Pre-Requisites / Co-Requisites

- Undergraduate course in digital design
- Undergraduate course in linear algebra
- EEE 5716: Introduction to Hardware Security and Trust (or permission of instructor)
- Students should have some basic familiarity with VHDL, Verilog, and CAD/EDA tools

Course Objectives
This is a graduate-level course that intends to help students

- Familiarize themselves with current state-of-the-art in hardware security – physical unclonable functions (PUFs), hardware Trojan detection and prevention, side channel analysis, physical attacks, through lectures
- Understand important topics not covered in the Introductory course such as hardware obfuscation, logic locking, split manufacturing, circuit camouflaging, IP encryption, security design rules, security-aware CAD/EDA tools and flows, quantum computing, and more through lectures, assignments, and projects
- Learn about the foundations of quantum computing, its important applications in security, and its impact on cryptography
- Master a variety of commercial and open-source CAD/EDA tools such as Synopsys Design Compiler, Synopsys TetraMax,, Berkley's ABC, etc. by attending TA-led lectures and viewing pre-recorded tutorials/demos and completing assignments
- Improve technical communication skills by articulating the details of existing work as well as their own proposed techniques through class participation, quizzes, and presentations

Materials and Supply Fees
N/A

Required Textbooks and Software

N/A

Recommended Materials

i. D. Forte, S. Bhunia, and M. Tehranipoor. *Hardware Protection through Obfuscation*, Springer, 2017.
ii. S. Bhunia and M. Tehranipoor. *Hardware security: a hands-on learning approach*. Morgan Kaufmann, 2018.
iii. C. Bernhardt. *Quantum computing for everyone*. MIT Press, 2019.
iv. List of reference papers provided in each slide deck

Course Schedule

Wk	Date	Topics
1	8/22-8/28	Syllabus, course overview, and ethics; Overview of emerging challenges, applications, and new nanoscale tools/technologies; Discussion of assignment expectations (requirements, deliverables, etc.)
		IP PROTECTION AND HARDWARE OBFUSCATION
2	8/29-9/4	Introduction to IP protection, motivation, and applications; Hardware obfuscation methods and metrics: Introduction to keyed combinational locking; Logic locking methods, attacks, and countermeasures
3	9/5-9/11	Logic locking methods, attacks, and countermeasures continued; Keyed combinational locking (analog, cyclic, and scan chain) methods, attacks, and countermeasures
		Assignment #1- TCL, Design Compiler, and ABC [+ Insert key gates]
4	9/12-9/18	Sequential (FSM) locking methods; PCB locking/obfuscation, attacks, and countermeasures; Keyless obfuscation methods (IC camouflaging, split manufacturing, 2.5D/3D-IC based, and post-manufacturing edit)
		Quiz #1- Week 2-3 Material
5	9/19-9/25	Keyless obfuscation methods continued; Built-in self-authentication (BISA) and obfuscated BISA (OBISA)
6	9/26-10/2	Review of cryptographic primitives and protocols; P1735 standard for IP encryption and vulnerabilities;
		Assignment #2- VCS and TetraMax [+ Compute corruptibility and SCOAP for logic locked netlist]
7	10/3-10/9	Introduction to Secure Multi-Party Computation, Garbling and Oblivious Transfer; Garbled EDA; Summary of IP protection
		Quiz #2- Week 6 Material
		CURRENT STATE-OF-THE-ART IN HARDWARE SECURITY
8	10/10-10/16	SoTA in design tools for side channel aware implementations

9	10/17-10/23	SoTA in physical attacks and countermeasures: IC probing and fault injection (FI) attacks; RAM-Jam; Probing and FI metrics and assessment; Anti-probing/FI solutions and limitations; iPROBE (CAD for anti-probing);
10	10/24-10/30	SoTA in counterfeit detection and avoidance
		Quiz #3- Weeks 8-9 Material
11	10/31-11/6	SoTA in physical unclonable functions
		Assignment #3 – Primetime [Inject faults and/or collect power traces]
		EMERGING TOPICS IN HARDWARE SECURITY
12	11/7-11/13	Introduction to quantum computing; Quantum gates and circuits
13	11/14-11/20	Quantum applications, simulations, and EDA; Quantum algorithms
		Quiz #4- Weeks 10-11 Material
14	11/21-11/27	**THANKSGIVING HOLIDAY**
15	11/28-12/4	Physical security in the post-quantum era; Extra-credit presentations
16	12/5-12/17	Extra-credit presentations
17	12/12-12/16	Quiz #5 - Quantum computing

Red indicates student deliverable

Attendance Policy, Class Expectations, and Make-Up Policy

This class will be presented online using Zoom and requires access to a working webcam and stable internet connection. I prefer that students keep their camera on during the class so that I can see you as I would during normal face-to-face classes. Studies show that if we can see each other's faces then we will have more engagement, more student success, and more faculty success. However, this is not a requirement. I understand if on certain days you can't have your camera on due to internet bandwidth limitations, other family members, health issues, or any other reasons.

In addition, the instructor expects students to

- Develop novel slides, assignment solutions, etc., i.e., you are not allowed to use <u>any</u> prior project or research material (even their own) as part of the course projects or assignments. This will be considered cheating and will be dealt with in a severe manner. *See Section on Honesty Policy.*
- Follow the presentation and assignment guidelines provided by the instructor and TAs, including use of the Microsoft Word, Powerpoint, and Latex templates.
- Submit all their assignments, reports, tools, slides, etc. in a timely manner on Canvas. 5% credit will be subtracted per day beyond the submission deadline of any assignment/project materials (assuming instructor did not provide permission)

- Present your results, demo, etc. in their entirety within the specified timeslot

Excused absences must be in compliance with university policies in the Graduate Catalog (http://gradcatalog.ufl.edu/content.php?catoid=10&navoid=2020#attendance) and require appropriate documentation.

Evaluation of Grades

- Class Participation 14%
- CAD/EDA Assignments 36%
- Quizzes 50%

Grading Policy

Percent	Grade	Grade Points
93.4 - 100	A	4.00
90.0 - 93.3	A-	3.67
86.7 - 89.9	B+	3.33
83.4 - 86.6	B	3.00
80.0 - 83.3	B-	2.67
76.7 - 79.9	C+	2.33
73.4 - 76.6	C	2.00
70.0 - 73.3	C-	1.67
66.7 - 69.9	D+	1.33
63.4 - 66.6	D	1.00
60.0 - 63.3	D-	0.67
0 - 59.9	E	0.00

More information on UF grading policy may be found at:
http://gradcatalog.ufl.edu/content.php?catoid=10&navoid=2020#grades

Students Requiring Accommodations

Students with disabilities who experience learning barriers and would like to request academic accommodations should connect with the disability Resource Center by visiting https://disability.ufl.edu/students/get-started/. It is important for students to share their accommodation letter with their instructor and discuss their access needs, 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/.

In-Class Recording

Students are allowed to record video or audio of class lectures. However, the purposes for which these recordings may be used are strictly controlled. The only allowable purposes are (1) for

personal educational use, (2) in connection with a complaint to the university, or (3) as evidence in, or in preparation for, a criminal or civil proceeding. All other purposes are prohibited. Specifically, students may not publish recorded lectures without the written consent of the instructor.

A "class lecture" is an educational presentation intended to inform or teach enrolled students about a particular subject, including any instructor-led discussions that form part of the presentation, and delivered by any instructor hired or appointed by the University, or by a guest instructor, as part of a University of Florida course. A class lecture does not include lab sessions, student presentations, clinical presentations such as patient history, academic exercises involving solely student participation, assessments (quizzes, tests, exams), field trips, private conversations between students in the class or between a student and the faculty or lecturer during a class session.

Publication without permission of the instructor is prohibited. To "publish" means to share, transmit, circulate, distribute, or provide access to a recording, regardless of format or medium, to another person (or persons), including but not limited to another student within the same class section. Additionally, a recording, or transcript of a recording, is considered published if it is posted on or uploaded to, in whole or in part, any media platform, including but not limited to social media, book, magazine, newspaper, leaflet, or third party note/tutoring services. A student who publishes a recording without written consent may be subject to a civil cause of action instituted by a person injured by the publication and/or discipline under UF Regulation 4.040 Student Honor Code and Student Conduct Code.

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/process/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
- Jennifer Nappo, Director of Human Resources, 352-392-0904, jpennacc@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

Campus Resources:
Health and Wellness

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 Connections 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: https://distance.ufl.edu/state-authorization-status/#student-complaint