

Advanced Hardware Security and Trust

EEE 6742

Class Periods: T, 8-9, 3:00PM-4:55PM; R, 9, 4:05PM-4:55PM

Location: Online

Academic Term: Fall 2020

Instructor:

Name: Dr. Domenic Forte
Email: dforte@ece.ufl.edu
Telephone: 352-392-1525
Office Hours: By appointment (Zoom)

Teaching Assistant/Peer Mentor/Supervised Teaching Student:

Please contact through the Canvas website

- Sarah Amir, sarah.amir@ufl.edu

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.
- 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, counterfeit electronics detection and avoidance, etc. through lectures, student-led presentations, and literature surveys
- Understand important topics not covered in the Introductory course such as hardware obfuscation, logic locking, split manufacturing, circuit camouflaging, IP encryption, security design rules, information flow tracking, security-aware CAD/EDA tools and flows, and more through lectures, assignments, and projects
- Perform a literature survey and prepare a presentation on one of these advanced topics
- Master a variety of commercial and open-source CAD/EDA tools such as Synopsys Design Compiler, Synopsys TetraMax, MiniSAT and CryptoMiniSAT satisfiability solvers, Cadence JasperGold Formal Verification, Berkley's ABC, CU Decision Diagram (CUDD) package, and BDS BDD-based Logic Synthesis System by attending TA-led lectures and viewing pre-recorded tutorials/demos
- Prepare for participation in hardware security competitions
- Demonstrate proficiency with several CAD/EDA tools by completing research projects in topics provided by the instructor (or other topics with the instructor's permission)

Improve technical communication skills by articulating the details of existing work as well as their own proposed techniques through reports 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. P. Mishra, S. Bhunia, and M. Tehranipoor, *Hardware IP Security and Trust*, Springer, 2016.
- iv. M. Tehranipoor, U. Guin, and D. Forte, *Counterfeit Integrated Circuits: Detection and Avoidance*, Springer, 2015
- v. List of papers provided on the course website

Course Schedule

Wk	Date	Topics
1	8/31-9/6	Syllabus, course overview, and ethics; Overview of emerging challenges, applications, and new nanoscale tools/technologies; Discussion of Project and Presentation Expectations (Requirements, deliverables, etc.); Overview of commercial and open-source CAD/EDA tools and scripts (BDD, ATPG, etc.)
		CAD/EDA tools assignment released
		IP PROTECTION AND HARDWARE OBFUSCATION
2	9/7-9/13	Introduction to IP protection, motivation. and applications; Hardware obfuscation methods and metrics: Keyed combinational locking (logic, cyclic, and scan chain) methods, attacks, and countermeasures
3	9/14-9/20	Sequential (FSM and best possible) locking methods; Delay locking; LUT locking; BDD locking; Error-tolerant obfuscation; PCB locking/obfuscation, attacks, and countermeasures;
4	9/21-9/27	Keyless obfuscation methods (IC camouflaging, split manufacturing, 2.5D/3D-IC based, and post-manufacturing edit); Built-in self-authentication (BISA) and obfuscated BISA (OBISA); Synthetic benchmark generation for hardware obfuscation
		CAD/EDA tools assignment (HW # 1) due; Formation of Groups for Project and Presentation
5	9/28-10/4	Review of cryptographic primitives and protocols; P1735 standard for IP encryption and vulnerabilities; FORTIS-based IP protection, and obfuscation key management; Summary of hardware obfuscation
		EMERGING TOPICS IN HARDWARE SECURITY
6	10/5-10/11	Internet-of-things (IoT) and application domains; Fundamental technologies and design methods; Security issues and SW/HW based attacks (E.g., Ransomware, Rowhammer); IoT case studies and lessons learned
7	10/12-10/18	Analog-and-mixed signal (AMS) chip properties; Security opportunities and challenges; AMS PUFs; Analog logic locking and attacks; AMS-enabled security (side channel attestation and lightweight crypto); FPGA properties and vulnerabilities; FPGA countermeasures and solutions; Emerging issues in FPGA (use in data centers; reconfigurability);
		Project assignment (HW # 2) due

8	10/19-10/25	Security Design Rule Check motivation and examples (FSM vulnerabilities and countermeasures); Information flow security and tracking; Gate level information flow tracking (GLIFT) and use; Flow-based hardware Trojan detection
9	10/26-11/1	IC probing and fault injection (FI) attacks; Probing and FI metrics and assessment; Anti-probing/FI solutions and limitations; iPROBE (CAD for anti-probing);
		Presentation from two student groups (TBD)
10	11/2-11/8	Emerging technologies, physics, and security challenges/opportunities: Phase change memory, memristors, spintronic devices, graphene and carbon nanotube, Si nanowire, and finFET
		Project assignment (HW # 3) due
		Presentation from two student groups (TBD)
		CURRENT STATE-OF-THE-ART IN HARDWARE SECURITY
11	11/9-11/15	General hardware Trojans and new Trojans (dopant-level, analog, and FPGA); Vulnerability metrics and benchmarking at RTL, gate, and layout level; Hardware Trojan prevention taxonomy; EM-based Trojan detection
		Presentation from two student groups (TBD)
12	11/16-11/22	State-of-the-art in counterfeit detection and avoidance; Aging-based statistical fingerprints and detection: ERF, CTS, Memory-based, FPGA-RO-based, and LDO-based; CDIR design and optimization; Introduction to physical attacks and equipment
		Presentation from two student groups (TBD)
13	11/23-11/29	THANKSGIVING HOLIDAY
		Project assignment (HW # 4) due
14	11/30-12/6	New PUF designs (CMOS, CNT, and RRAM/memristor); Virtual proofs of reality; Non-invasive attacks on strong PUFs: modeling attacks, side channel attacks, PAC learning, and optimization-theoretic; Countermeasures: One time use, Erasable/controlled PUF, and Lockdown techniques
		Presentation from two student groups (TBD)
15	12/7-12/9	State-of-the-art in semi-invasive and non-invasive attacks: Optical and laser imaging, fault injection (UV, photon injection, and local heating), and side channel attacks (optical emission and induced leakage); Examples of attacks on FPGA black keys, CPLD logic and primitives, and PUFs (SRAM, RO, and Arbiter)
16	12/12-12/18	Final project presentations/demos and final research paper due

Red indicates student deliverable

Purple indicates TA led

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, students are expected to

- Be punctual and attend all lectures for class participation.
- Develop novel slides, project solutions, and reports, i.e., you are not allowed to use any 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 report 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

- Assignments and Quizzes 40%
- Class Presentation 20%
 - Organization (30%)
 - Quality of Slides (20%)
 - Clarity (30%)
 - Q&A (20%)
- Final Project Deliverables 35%
 - Successful Demo (40%)
 - Code Commenting/Documentation/Usability (10%)
 - Final Paper (40%)
 - Bonus (up to 20%)
- Class Participation (~0.33% per week) 5%

Grading Policy

Percent	Grade	Grade Points
90.0 - 100.0	A	4.00
87.0 - 89.9	A-	3.67
84.0 - 86.9	B+	3.33
81.0 - 83.9	B	3.00
78.0 - 80.9	B-	2.67
75.0 - 79.9	C+	2.33
72.0 - 74.9	C	2.00
69.0 - 71.9	C-	1.67
66.0 - 68.9	D+	1.33
63.0 - 65.9	D	1.00

60.0 - 62.9	D-	0.67
0 - 59.9	E	0.00

More information on UF grading policy may be found at:
<https://catalog.ufl.edu/ugrad/current/regulations/info/grades.aspx>

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 feedback on the quality of instruction in this course by completing online evaluations at <https://evaluations.ufl.edu/evals>. Evaluations are typically open during the last two or three weeks of the semester, but students will be given specific times when they are open. Summary results of these assessments are available to students at <https://evaluations.ufl.edu/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://www.dso.ufl.edu/sccr/process/student-conduct-honor-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: <http://registrar.ufl.edu/catalog0910/policies/regulationferpa.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: <http://www.counseling.ufl.edu/cwc>, 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](mailto:title-ix@ufl.edu), 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 support, 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://www.crc.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://www.dso.ufl.edu/documents/UF_Complaints_policy.pdf.

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