Advanced Hardware Security and Trust
EEE 6742
Class Periods: T, 10, 5:10PM-6PM; R, 10-11, 5:10PM-7:05PM
Location: BEN0328
Academic Term: Fall 2018

Instructor:

Name: Dr. Domenic Forte
Email: dforte@ece.ufl.edu
Telephone: 352-392-1525
Office Hours: Tuesdays, 9:00AM-11AM, MAE226D

Teaching Assistant:

Name: Huanyu Wang
Email: huanyuwang@ufl.edu
Office Hours: 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.
- 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 discuss emerging topic areas associated with security challenges and opportunities of nanoscale devices (memristor, phase change memory, graphene, etc.), 2.5D/3D integration, Internet of Things (IoT), analog and mixed signal ICs, FPGAs, and non-electronics supply chain
- 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. P. Mishra, S. Bhunia, and M. Tehranipoor, *Hardware IP Security and Trust*, Springer, 2016.
iii. M. Tehranipoor and C. Wang, *Introduction to Hardware Security and Trust*, Springer, 2011
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	8/22-8/26	Syllabus, course overview, and ethics; Overview of emerging challenges, applications, and new nanoscale tools/technologies; Introduction to IP protection, motivation. and applications
		IP PROTECTION AND HARDWARE OBFUSCATION
2	8/27-9/2	Hardware obfuscation methods and metrics: Combinational logic locking and IC camouflaging; Attacks and countermeasures
	8/30	Choose paper to present (associated project comes with it)
3	9/4-9/9	Sequential obfuscation methods: FSM-based obfuscation; Structural obfuscation; Split manufacturing; Built-in self-authentication (BISA) and obfuscated OBISA; 2.5D/3D-IC based obfuscation; Chip Editor
4	9/10-9/17	Discussion of Project (Requirements, deliverables, etc.); Overview of commercial and open-source CAD/EDA tools and scripts (BDD, ATPG, etc.); Formation of groups for Project 1
5	9/17-9/23	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
	9/20	Paper Presentations (see list of papers and projects)
	TBD	Possible Quiz on Hardware Obfuscation
		EMERGING TOPICS IN HARDWARE SECURITY
6	9/24-9/30	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
	9/25	Project Proposal due
	9/27	Tool Assignment Due

7	10/1-10/7	Analog-and-mixed signal (AMS) chip properties; Security opportunities and challenges; AMS PUFs; 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)
	10/2	Weekly Project Status Update #1
8	10/8-10/14	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
	10/9	Weekly Project Status Update #2
9	10/15-10/21	IC probing attacks; Probing metrics and assessment; Anti-probing solutions and limitations; iPROBE (CAD for anti-probing); Tamper metrics and assessment; anti-tamper solutions
	10/16	Weekly Project Status Update #3
10	10/22-10/28	Emerging technologies, physics, and security challenges/opportunities: Phase change memory, memristors, spintronic devices, graphene and carbon nanotube, Si nanowire, and finFET
	10/23	Weekly Project Status Update #4
	TBD	Possible Quiz on Emerging Topics
		CURRENT STATE-OF-THE-ART IN HARDWARE SECURITY
11	10/29-11/4	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
	10/30	Weekly Project Status Update #5
	11/1	Mid-semester Project Deliverables due
12	11/5-11/11	State-of-the-art in counterfeit detection and avoidance; Aging-based statistical fingerprints and detection: ERF, CTS, Memory-based, and FPGA-RO-based; CDIR design and optimization; Introduction to physical attacks and equipment
	11/6	Weekly Project Status Update #6
13	11/13-11/18	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
	11/13	Weekly Project Status Update #7
14	11/19-11/20	**THANKSGIVING HOLIDAY**
	11/20	Weekly Project Status Update #8
15	11/26-12/2	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)
	11/27	Weekly Project Status Update #9
	TBD	Possible Quiz on State-of-the-Art

16	12/3-12/5	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

Students are expected to

- Be punctual and attend all lectures.
- 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 final course project. 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
- Present your results, demo, etc. in their entirety within the specified timeslot

Excused absences are consistent with university policies in the undergraduate catalog (https://catalog.ufl.edu/ugrad/current/regulations/info/attendance.aspx) and require appropriate documentation.

Evaluation of Grades

- Assignments and Quizzes 10%
- Proposal (7%) and Project Status Updates (2% per week, weeks 7-15) 25%
- Mid-semester Project Deliverables 25%
  - Progress Report (50%)
  - Successful Demo (50%)
- Final Project Deliverables 35%
  - Final Research Paper (50%)
  - Successful Demo (25%)
  - Presentation (25%)
- Class Participation (~0.33% per week) 5%

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:
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.

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:

If you or a friend is in distress, please contact umatter@ufl.edu or 352 392-1575 so that a team member can reach out to the student.

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 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.