Advanced Hardware Security and Trust
EEL 6935 Section 1500
Class Periods: T, 10, 5:10PM-6PM; R, 10-11, 5:10PM-7:05PM
Location: MAEB238
Academic Term: Fall 2017

Instructor:

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

Teaching Assistants:

1) Bicky Shakya, bshakya@ufl.edu, MAE119
2) Adib Nahiyan, adib1991@ufl.edu, MAE 119

Course Description

The end of Moore's law as we know it is changing the landscape of integrated circuit (IC) design and fabrication. In parallel, the threat space in hardware security is always rapidly evolving. This course expands on the foundational knowledge and concepts provided by the Introduction to Hardware Security and Trust course in order to understand and investigate these new challenges. The first portion of the course will include topics related to opportunities/challenges with respect to emerging nanoscale technologies, integration approaches, EDA tools, and application spaces. The second portion shall cover the current state-of-the-art research in hardware security primitives, attacks, and countermeasures. *Lecture. Credits 3.*

Course Pre-Requisites / Co-Requisites

- EEL 4712C: Digital Design (or equivalent)
- EEL 5934: Introduction to Hardware Security and Trust (or permission of instructor)
- Students should have familiarity with VHDL, Verilog, and EDA tools for simulation, synthesis, layout, etc. from at least one of the well-known vendors (Synopsys, Cadence, or Mentor Graphics).

Course Objectives

This is a graduate-level advanced topics 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. (allowing much greater depth than the Introductory course)
- 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.
- 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
- Develop hands-on experience with a variety of commercial and open-source CAD/EDA tools such as Synopsys Design Compiler, Synopsys TetraMax, MiniSAT and CryptoMiniSAT satifisability solvers, Cadence JasperGold Formal Verification, Berkley's ABC, CU Decision Diagram (CUDD) package, and BDS BDD-based Logic Synthesis System
- Prepare for participation in hardware security competitions
- Be capable of research in any course topic and complete a research project in hardware obfuscation (or another topic with permission of instructor)

- Improve technical communication skills by articulating the details of existing work as well as their own proposed techniques through reports and presentations

Course Structure

The majority of lectures will be prepared and delivered by the instructor and/or TAs. The remaining lecture periods will be used to discuss project approaches and results – in the form of informal discussions as well as formal presentations. All students are expected to participate in group discussion during all lectures and presentations. When presentation are given by students, scores on the presentation will be determined by students in attendance, TAs, and instructor. There will be two group projects – **Project 1:** Students will participate in a pilot competition on logic locking and hardware obfuscations. Obfuscated/locked benchmarks will be provided to students who will attack them using approaches discussed in class. Students give a demo and short presentation detailing their results and figures of merit. They will also provide feedback to the TAs and instructor about challenges/issues encountered during the project; and **Project 2:** An end-of-semester course project on one of the topics described below, or proposed by the group. Each group will demonstrate their tools (if applicable), provide a progress report, write a 6 page research paper, and present their approach/results during the last week of class.

Students who are interested in fulfilling **MS NON-THESIS EXAM** requirements can do so by completing an additional assignment from the instructor. Students must register online to take the MS Exam and inform the instructor of their registration. The assignment consists of summarizing a recent paper related to hardware security selected by the student and approved by the instructor.

Materials and Supply Fees

N/A

Recommended Textbooks and Software

i. M. Tehranipoor and C. Wang, Introduction to Hardware Security and Trust, Springer, 2011
ii. M. Tehranipoor, U. Guin, and D. Forte, Counterfeit Integrated Circuits: Detection and Avoidance, Springer, 2015
iii. P. Mishra, S. Bhunia, and M. Tehranipoor, Hardware IP Security and Trust, Springer, 2016.
iv. D. Forte, S. Bhunia, and M. Tehranipoor, Hardware Protection through Obfuscation, Springer, 2017.

Recommended Reading

See list provided on the course website

Attendance Policy, Class Expectations, and Make-Up Policy

Students are expected to

- Be <u>punctual</u> and attend all lectures. If missing class is unavoidable, prior permission must be requested from the instructor. If such permissions are not requested or not granted, the student will receive a <u>score of zero</u> for class participation during the missed class (NO EXCEPTIONS).
- Develop novel slides, project solutions, and reports, i.e., they are not allowed to use <u>any</u> 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 reports, tools, slides, etc. in a timely manner on Canvas
- Present their results, demo, etc. in their entirety <u>within the specified timeslot</u>

Course Schedule

Wk	Date	Topics
1	8/21-8/25	Syllabus, course overview, and ethics; Brief review of hardware security and trust topics; Limitations of existing approaches; Overview of emerging challenges, applications, and new nanoscale technologies
		HARDWARE OBFUSCATION
2	8/28-9/1	Introduction to hardware obfuscation motivation and applications; Obfuscation metrics; Logic locking and IC camouflaging; Attacks on logic locking and countermeasures
3	9/4-9/8	Discussion of Project 1 (Requirements, deliverables, etc.); Overview of tools and scripts (BDD, ATPG, etc.); Formation of groups for Project 1 (Bicky and Adib)
4	9/11-9/15	FSM-based obfuscation; Structural obfuscation; Split manufacturing; BISA and OBISA; 2.5D/3D-IC based obfuscation
5	9/18-9/22	P1735 IP Encryption, FORTIS, and obfuscation key management; Summary of hardware obfuscation and promising new approaches such as Chip Editor
		EMERGING TOPICS IN HARDWARE SECURITY
6	9/25-9/29	Internet-of-things (IoT) applications and challenges
7	10/2-10/6	AMS security issues; AMS-enabled security; FPGA security
8	10/9-10/13	Project 1 presentations and deliverables due
9	10/16-10/20	Emerging technologies and security applications (Bicky)
10	10/23-10/27	Security Design Rule Check motivation and examples (FSM vulnerabilities and countermeasures); Information flow security and tracking; GLIFT; Flow-based hardware Trojan detection (Adib)
	10/27	Formation of Project 2 Groups; Proposal due for Project 2
		CURRENT STATE-OF-THE-ART IN HARDWARE SECURITY
11	10/30-11/3	New PUF designs (CMOS and emerging); Attacks and countermeasures on strong PUFs (Bicky)
	11/3	Non-Thesis Final Exam in Advanced Hardware Security and Trust *(Interested MS students only)*
12	11/6-11/10	General hardware Trojans and new Trojans; Vulnerability metrics and benchmarking; Hardware Trojan prevention + related (Adib)
	11/10	Project 2 progress reports due
13	11/13-11/17	State-of-the-art in counterfeit detection and avoidance; State-of-the-art in physical attacks
14	11/20-11/24	**THANKSGIVING HOLIDAY**
15	11/27-12/1	State-of-the-art in physical attacks; Physical attacks on PUFs
	11/30	Final presentations/demos
16	12/4-12/8	Final presentations/demos
17	12/11-12/15	Final research paper due

Red indicates student deliverable
Blue indicates lectures led by TAs

Recommended Topics for Final Project (i.e., Project 2)

- *Logic Locking and Hardware Obfuscation*
  - Develop a new logic locking approach and/or attack countermeasure; Demonstrate on ten benchmarks; Compare with existing approaches
  - Develop new structural attacks on any existing logic locking and/or hardware obfuscation approach; Demonstrate them on ten benchmarks; Compare with existing functional attacks
  - Develop one or more attacks on FSM locking and/or obfuscation; Demonstrate them on the benchmarks on Trust-HUB.org
  - Develop new metrics and use them to create a synthetic logic locking / hardware obfuscation benchmark generation tool; Generate ten new benchmarks, obfuscate them and attack them; Report area overhead, attack time, etc.
- *Analog and Mixed Signal (AMS) and FPGA Security*
  - Develop methods to lock and obfuscate AMS chips; Explain the advantages of your methods and what types of AMS chips they apply to
  - Develop hardware Trojan triggers and payloads suitable for different types of AMS chips
  - Investigate the security threats surrounding the FPGA multi-tenant usage model; Propose and demonstrate threats and mitigations on a real FPGA platform
  - Develop one or more secure secret key exchange protocols for FPGA bitstream encryption; Implement and demonstrate them on an FPGA platform of your choice.
- *Emerging Devices*
  - Develop a new hardware obfuscation technique/tool based on emerging device/integration
  - Develop a new hardware Trojan based on emerging device/integration
  - Develop one or more anti-counterfeit mechanisms based on emerging devices; Describe their concept of operation and what types of counterfeits they can detect
- *Security Design Rule Check*
  - Develop a framework to analyze violations of information flow security policies in a hardware design. Demonstrate the effectiveness of the framework using benchmarks (application of Jasper tool is not allowed for this project)
  - Develop a framework to quantitatively evaluate how vulnerable a hardware design is to side channel attacks (any modality). Demonstrate the effectiveness of the framework using benchmarks.
  - Develop a framework to quantitatively evaluate how vulnerable a hardware design is to fault injection attacks (one or more methods). Demonstrate the effectiveness of the framework using benchmarks.
  - Demonstrate how CAD tools (high level synthesis tools/ RTL to gate level synthesis tools) can introduce vulnerabilities (information flow leakage/side channel leakage) in a hardware design.
- *Physical Unclonable Function (PUF)*
  - Implement a suite of tools that efficiently evaluates a weak PUF's uniqueness, reliability, and randomness; Extend the above tools to strong PUF evaluation; Implement at least two machine learning approaches from the literature on a strong PUF
- *Hardware Trojan Detection and Prevention*
  - Develop a tool that automatically inserts sequentially triggered hardware Trojans into RTL, netlist or layout levels; Demonstrate on several benchmarks, including one large benchmark; Develop a metric that evaluates the ability of an attacker to detect your Trojans
  - Apply machine learning and/or formal verification techniques to detect hardware Trojans inserted at RTL level before and after synthesis

Evaluation of Grades

- Project 1 (Obfuscation Competition) 35%
  - Successful Demo (20%)
  - 10 Minute Presentation (40%)
  - Quality of Results (20%)
  - Project Feedback (20%)
  - Potential Bonus[1] (20%)
- Project 2 (Final Project) 50%
  - Progress Report (20%)
  - Successful Demo (20%)
  - Presentation (20%)
  - Final Research Paper (40%)
- Class Participation (1% per week) 15%

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/.

[1] Bonus will be rewarded to groups if their project contains significant novelty in the implementation and/or attacks.

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.