EEL 6935 CAD for Hardware Security Validation

Class periods: Tuesdays, Period 10, 5:10 PM – 6:00 PM
Thursdays, Period 10-11, 5:10 PM – 7:05 PM
Location: LAR 0239
Academic Term: Spring 2020

Instructor:
Dr. Farimah Farahmandi
farimah@ece.ufl.edu
352-392-0910
Office Hours: TBD

Teaching Assistants:
Please contact through the Canvas website

- TBD (XXX@ufl.edu, Office Hours: TBD)
- TBD (XXX@ufl.edu, Office Hours: TBD)
-

Course Description:

Catalog description: **Credits 3**;
The course will provide an overview of the SoC design flow for FPGA and ASIC designs. Moreover, it teaches various hardware verification/validation techniques (e.g., simulation-based validation, formal methods, and hybrid approaches) using several computer-aided design (CAD) tools in pre- and post-silicon stages. The course also outlines the challenges in hardware security verification/validation and overview various techniques/tools to detect information leakage, side-channel leakage, malicious modifications, fault-injection attacks, and intellectual property (IP) piracy.

Hardware Validation and Verification, Hardware Security, CAD tools, Formal Methods, Simulation-based Validation, and Test Generation.

Course Pre-Requisites / Co-Requisites:
Co-requisites with Introduction to Hardware Security and Computer Architecture. Students are expected to have a general background in Digital Design also be experienced with Verilog/VHDL programming. Students can bypass co-requisites with permissions.

Course Objectives:
Hardware Validation is a major bottleneck such that more than 70% of design efforts are dedicated to verification and validation efforts in pre-silicon and post-silicon stages. Verification/validation has several objectives, such as ensuring correct functionality, timing, reliability, security and trust assurance, etc. Security validation/verification is critical since it aims to detect any intentional/unintentional security vulnerabilities that lead to the leakage of sensitive information in design as well as the denial of service. Security validation is challenging due to the stealthy nature of potential attacks, as well as the diverse nature of vulnerabilities in system-on-chip (SoC) designs. This course will teach various design and verification techniques for hardware designs using existing techniques and methodologies in different stages of a design life-cycle as well as various abstraction levels (e.g., high-level C/C++, register transfer level,

gate-level, and layout level). The challenges and limitations of each of the techniques will also be discussed. In the second half of the design, the discussed techniques and tools will be used to identify the design weaknesses that cause the security vulnerabilities (e.g., information leakage, side-channel leakage, fault-injection attacks, malicious modifications, and IP piracy) in various case studies. We will use commercial CAD tools and academic techniques to detect such vulnerabilities in SoC designs. Some countermeasures also will be discussed.
Upon the completion of the course, students should have a good understanding of the following topics:

SoC Design Flow (FPGA and ASIC)
Verification/validation techniques
Verification/validation objectives, tools, metrics, and benchmarks

- Pre-silicon Validation approaches
- Post-silicon validation approaches

Why is Security Validation needed? (1 week)

- Security Verification challenges
- Threat models
- Trust/security metrics and benchmarks

CAD for Security Assessment and countermeasures

- Information leakage (high-level, RTL, gate-level)
- Side-channel leakage (high-level, RTL, gate-level, layout)
- Fault injection attacks (high-level, RTL, gate-level)
- Malicious modifications (high-level, RTL, gate-level, layout)
- IP Piracy (bitstream protection/ tampering analysis, and Reverse engineering)

Materials and Supply Fees
None
Equipment
None

Required Textbooks and Software

- **Textbook:** No textbook. Relevant research papers, slides, and other notes will be provided in class.
- **Software:** Xilinx ISE package, Synopsys Verilog simulation package and Formal Tools, Cadence Design System, Programming and Scripting Software (Matlab, Python, C/C++)

Course Schedule

Week	Topics	Notes
1, 2	SoC Design Flow for ASIC and FPGA	Course Intro, Design Integration, Synthesis, Design for test and debug insertion, Layout Extraction, Manufacturing, …
3, 4	Verification/validation Objectives	- Timing, functionality, design constraints (power, energy, area), security, reliability - Verification benchmarks
5, 6, 7	Pre-silicon Validation	- Metrics - Simulation-based validation techniques (random test generation, directed test generation, constraint-random tests, UVM/OVM) + tools - Formal methods (equivalence checking, model checking, theorem proving, satisfiability problems) + tools - Statistical approaches + tools - Machin learning based approaches - ***Assignment 1 Due Week 6***
8	Post-silicon Validation	- Metrics - Design for test + tools - Design for debug + tools - Machine learning based approaches - ***Assignment 2 Due Week 8***
9	Why is security validation needed?	- Security Verification challenges - Threat models - Trust/security metrics and benchmarks - Intro to CAD for Security Assessment and countermeasures
10, 11	Information leakage	- Tools (E.g., Vivado and Catapult), - Abstraction levels high-level (C/C++), RTL, gate-level - Sample countermeasures - ***Student in class presentations***
12,13	Side-channel leakage Malicious Modifications	- Tools, Abstraction levels high-level (C/C++), RTL, gate-level, layout-level - Sample countermeasures - ***Student in class presentations***
14, 15	Fault-injection Attacks Reverse Engineering	- Tools, Abstraction levels high-level (C/C++), RTL, gate-level, layout-level - Sample countermeasures - Obfuscation, bitstream protection and tampering analysis, …

		- ***Student in class presentations***
16	**Exam1 & Final Reports**	-

Attendance Policy, Class Expectations, and Make-Up Policy

On-time attendance in the class is mandatory. There are no make-up exams/quizzes unless there is an acceptable reason (illness, serious family emergencies, UF-imposed curriculum requirement or activity, religious holiday, or jury duty). In those cases, a make-up exam will be organized. Students should contact the instructor ahead of the exam so that an alternate exam schedule can be found. Students missing exams for unpredictable family or medical reasons should notify the instructor ahead of the exam time. If you miss more than one test, you will need to contact the instructor to evaluate whether you should pursue the class further or receive an incomplete. Students missing an exam without giving advance notice to the instructor, or without providing a valid (documented) reason, will receive a grade of F for this exam. Make-up will not be given for computer assignments. If you believe that you have a valid exam conflict, please send the information at least eight days in advance to the instructor. Please specify the times of your conflict and then times immediately before or after the scheduled exam time when you are available.

To ensure a classroom environment conducive to success for everyone, please turn off all cell phones before class starts. If you must enter the classroom late, be considerate, and be as quiet as possible. Persistent disruptive behavior will result in grade deductions.

All use of electronic devices during an exam will be considered a violation of the student honor code (i.e., cheating). Laptop computer and tablets are welcome in class as long as they are used for class-related work. Surfing the web, checking email, making posts, etc., is strictly prohibited.

Evaluation of Grades

Assignment	Total Points	Percentage of Final Grade
Final Exam	100	30%
Assignments (individual)	100 each	20%
In class presentation (team work)	100	20%
Final Paper Report (team work)	100	30%

The class presentation will be assigned by the instructor to teams of two students. Each team will be required to give a 45 minutes presentation on 3~5 papers on various hardware security validation/verification techniques that have been assigned to them. A 15 minutes Q&A will follow the presentation. The presentations will be graded based on the understanding of each of the students of the topic (50%), the ability to summarize the contributions of the papers and point to their limitations and challenges (30%), and the ability to answer questions during Q&A (20%). Each team member will be

graded individually for the part that they present, and the ability to answer the questions (50% of overall presentation grade). The students will be evaluated as a team for the quality of the slides and the overall presentation (50% of overall presentation grade).

The same team should write a final report on the presented papers. The students are expected to write a high-quality survey paper on the defined topic and assigned papers. The students are expected to look for other related papers and methods and include them in their reports. The report should contain:
(i) a comprehensive discussion on the motivation, related work, and background of the topic of research (20%);
(ii) a complete discussion on the technical details of reviewed approaches (25%);
(iii) a detailed comparison between reviewed approaches with stating their pros and cons as well as their limitation, correctness, and applicability of their results (25%);
(iv) the implementation the result of one of the reviewed methods (performed by the team members) (20%);
(v) conclusion and a discussion on the future possible directions (10%).

Each member should write a separate section in parts (iii) and (ii). The report should contain information on the contributions of each team member. Each team member will be graded as a team for parts i, iv, and v and individually for parts ii and iii.

Grading Policy

You will receive numerical grades for your quizzes and exams. The final grade will be determined primarily by the curve. The break between "B" and "B-" will be approximately set at the average of total scores of students with a score of %50 or more. Letter grades will be monotonic in the total course scores. Your grade will be solely based on your performance in the course and not on outside factors such as your wish to graduate this semester or the possibility of losing a scholarship.

In order to graduate, graduate students must have an overall GPA and a major GPA of 3.0 or better (B or better). Note: A "B-" average is equivalent to a GPA of 2.67, and therefore, it does not satisfy this graduation requirement. More information on UF grading policy may be found at: https://catalog.ufl.edu/graduate/regulations/

The following grading scale is subject to change

Percent	**Grade**	**Grade Points**
93- 100	A	4.00
89 - 92.9	A-	3.67
84 - 88.9	B+	3.33
81 - 83.9	B	3.00
78 - 80.9	B-	2.67
74 - 77.9	C+	2.33
71 - 73.9	C	2.00
65.0 - 70.9	C-	1.67
63 - 65.9	D+	1.33
60 - 62.9	D	1.00
58 - 59.9	D-	0.67
0 - 57.9	E	0.00

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." CHEATING WILL NOT BE TOLERATED. With the use of software, lab assignments as well as computer assignments and projects will be checked for the violation of the honesty and identification of unauthorized aids. If you are caught cheating on any assignment, project, quiz or exam, you will be prosecuted. There will be no negotiations and your case will be reported to the honor court. There are no excuses and no exceptions. 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

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**, 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://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.