# Syllabus for
# EEL 5934
# Introduction to Hardware Security and Trust
# Spring 2017

**1. Catalog Description**

Fundamentals of hardware security and trust for integrated circuits. Cryptographic hardware, invasive and non-invasive attacks, side-channel attacks, physically unclonable functions (PUFs), true random number generation (TRNG), watermarking of Intellectual Property (IP) blocks, FPGA security, counterfeit ICs, hardware Trojans in IP cores and ICs. Lecture. Credits 3.

**2. Pre-requisites**

**EEL3701C: Digital Logic (or equivalent)**

**3. Course Objectives**

This course will cover the following topics: Cryptographic processor and processing overhead analysis, physical and invasive attacks, side-channel attacks, physically unclonable functions, hardware-based true random number generators, watermarking of Intellectual Property (IP) blocks, FPGA security, passive and active metering for prevention of piracy, access control, hardware Trojan detection and isolation in IP cores and integrated circuits (ICs). The course is largely self-contained. Background on digital design would be sufficient. Introductory lectures will cover basic background on cryptography, authentication, secret sharing, VLSI design, test and verification. The main goals for this course are:

- Learning the state-of-the-art security methods and devices
- Integration of security as a design metric, not as an afterthought
- Protection of the design intellectual property against piracy and tampering
- Better understanding of attacks and providing countermeasures against them
- Detection and isolation of hardware Trojans
- Counterfeit Electronics: Detection and Prevention

**4. Instructors/coordinators:**


| | **Dr. Swarup Bhunia** | **Dr. Mark Tehranipoor** |
|---|---|---|
| Office Location | LAR 336A | BEN 325 |
| Office Hours | Wed 4-5pm | Mon 3-4pm |
| Telephone | 352-392-5989 | 352-392-2585 |
| Email | swarup@ece.ufl.edu | tehranipoor@ece.ufl.edu |
| Website | http://swarup.ece.ufl.edu | http://tehranipoor.ece.ufl.edu |


**5. Supervised Teaching Assistants (STAs)**


Tauhid Rahman: rahman.tauhid@ufl.edu

Fahim Rahman: fahim034@ufl.edu


The STAs will lead about half of the Thursday lectures and will assist with evaluation of student modules and final projects.

**6. Meeting Times**

| Days | Period | Time |
|---|---|---|
| Tuesday | 08-09 | 3:00-4:55PM |
| Thursday | 09 | 4:05-4:55PM |

**7. Meeting Location (for In-campus students)**

MAEB 0229

**8. Material and Supply Fees**

Avnet Spartan-6 LX9 MicroBoard for each project team ($~100/team) – each team may include up to 3 students

**9. Textbooks and Software Required**

**Textbook:** None

**Recommended Reference Book:**

M. Tehranipoor and C. Wang (Eds.), Introduction to Hardware Security and Trust, *Springer*, 2011

**Software:** Xilinx ISE package and Synopsys Verilog simulation package

**10. Recommended Reading and Videos**

*Reading*

- Mihir Bellare and Phil Rogaway, Introduction to Modern Cryptography
- Ross J. Anderson. Security Engineering: A guide to building dependable distributed systems. John Wiley and Sons, 2001
- Matt Bishop , Computer Security: Art and Science, Addison-Wesley, 2003
- William Stallings. Cryptography and Network Security, Fourth edition, 2007 (WS)
- The Hunt for the Kill Switch
- Hardware Trojan (computing)
- Defense Science Board Task Force On High Performance Microchip Supply
- Old Trick Threatens the Newest Weapons
- A Survey of Hardware Trojan taxonomy and Detection
- Detecting malicious inclusions in secure hardware: Challenges and Solutions
- FPGA Design Security Bibliography
- Supergeek pulls off 'near impossible' crypto chip hack
- Security through obscurity
- Trust-Hub

*Videos*

- What's inside a microchip? http://www.youtube.com/watch?v=GdqbLmdKgw4
- Zoom Into a Microchip http://www.youtube.com/watch?v=Fxv3JoS1uY8
- Public Key Cryptography: RSA Encryption: http://www.youtube.com/watch?v=wXB-V_Keiu8
- Counterfeit Electronics Could Be Dangerous, Funding Nefarious People http://www.youtube.com/watch?v=dbZiUe6guxc
- How Computers and Electronics Are Recycled http://www.youtube.com/watch?v=Iw4g6H7alvo
- Counterfeit Electronic Components Process http://www.youtube.com/watch?v=5vN_7NJ4qYA
- Counterfeit Inspection http://www.youtube.com/watch?v=MbQUvu2LN6o

- Gold from waste circuit electronics http://www.youtube.com/watch?v=ZkhOuNvkuu8
- Tarnovsky Deconstruct Processor https://www.youtube.com/watch?v=w7PT0nrK2BE

**11. Course Outline**

| Week | Tuesday Lecture | Instructor | Thursday Lecture | Instructor |
|---|---|---|---|---|
| Week 1 (Jan 5) | Syllabus, Ethics, Introduction to hardware security and trust, Emerging applications and the new threats | MT | Introduction to VHDL/Verilog I | STA |
| Week 2 (Jan 12, 14) | Introduction to Cryptography | SB | Introduction to VHDL/Verilog II | STA |
| Week 3 (Jan 19, 21) | Basics of VLSI Design and Test | MT | FPGA Tutorial I | STA |
| Week 4 (Jan 26, 28) | Security Based on Physically Unclonability and Disorder | SB | FPGA Tutorial II | STA |
| Week 5 (Feb 2, 4) | Hardware Metering | SB | Video Sessions | STA |
| Week 6 (Feb 9, 11) | Watermarking of HW IPs | SB | Video Sessions | STA |
| Week 7 (Feb 16, 18) | Physical Attacks and Tamper Resistance | MT | Video Sessions | STA |
| Week 8 (Feb 23, 25) | Security in Embedded Systems + **Midterm** | SB | Project Description | STA |
| Week 9 | SPRING BREAK | | | |
| Week 10 (Mar 8,10) | Fault Injection Attacks, Security of RFID Tags | SB | Student Presentations | SB/STA |
| Week 11 (Mar 15, 17) | Protecting against Scan-based Side Channel Attacks | SB | Student Presentations | SB/STA |
| Week 12 (Mar 22, 24) | Basics of PCB Security | SB | Student Presentations | SB/STA |
| Week 13 (Mar 29, 31) | Hardware Trojans: IC Trust (Taxonomy and Detection) | SB | Student Presentations | SB/STA |
| Week 14 (Apr 5, 7) | Counterfeit Detection and Avoidance | MT | Student Presentations | SB/STA |
| Week 15 (Apr 12, 14) | Hardware Trojans: IP Trust (Detection) + Design for Hardware Trust | SB | Student Presentations | SB/STA |
| Week 16 (Apr 19) | Side Channel Attacks and Countermeasures, Countermeasures for Embedded Microcontrollers | SB | Reading day | |

| Assignment Deadlines and Exam Dates | | | |
|---|---|---|---|
| **Week** | **Assignment** | **Group** | **Due Date** |
| Week 1 (Jan 5, 7) | TBD | N/A | TBD |
| Week 2 (Jan 12, 14) | TBD | N/A | TBD |
| Week 3 (Jan 19, 21) | TBD | N/A | TBD |
| Week 4 (Jan 26, 28) | TBD | N/A | TBD |
| Week 5 (Feb 2, 4) | TBD | N/A | TBD |
| Week 6 (Feb 9, 11) | TBD | N/A | TBD |
| Week 7 (Feb 16, 18) | TBD | N/A | TBD |
| Week 8 (Feb 23, 25) | Midterm Exam | N/A | February 23 |
| Week 9 | SPRING BREAK | | |
| Week 10 (Mar 8,10) | Group Paper Presentations | 1,2 | March 10 |

| | | | |
|---|---|---|---|
| Week 11 (Mar 15, 17) | Group Paper Presentations | 3,4 | March 17 |
| Week 12 (Mar 22, 24) | Group Paper Presentations | 5,6 | March 24 |
| Week 13 (Mar 29, 31) | Group Paper Presentations | 7,8 | March 31 |
| Week 14 (Apr 5, 7) | Group Paper Presentations | 9,10 | April 7 |
| Week 15 (Apr 12, 14) | Group Paper Presentations | 11,12 | April 14 |
| Week 16 (Apr 19) | Final Project | N/A | - |
| Week 17 | Final Exam | N/A | - |

**12. Attendance and Expectations**

***Format:*** The course is comprised of weekly lectures, 4-5 HW assignments, video sessions, student paper presentation module, and a final project. In addition, there will be two exams (midterm + final) and surprise pop quizzes.

Students must submit ***individual*** work ***individually*** on each module and as a team of 3 on final project. You are encouraged to work together on homework assignments and share ideas on lab assignments. However, you are not allowed to copy or duplicate any lab material (code, drawings, etc.) from another student. This work will be considered cheating and will be dealt with in a severe manner. See Section 19 on Honesty Policy.

The final project will require implementation of a hardware security primitive or attack on an FGPA based on several conference and journal papers distributed to the teams. The team's work will be evaluated through demonstration on several benchmarks. Each group will prepare a presentation, demonstration of the project, and final report. The final report will discuss challenges met, present in-depth analysis of the approaches implemented by the team, etc.

It is the student's responsibility to return all FGPA boards by the time of project demonstration.

**13. Grading-methods of evaluation**

- Exams 50% (10% quiz, 20% mid-term, 20% final)
- Project Demo/Report 15%
- Oral Presentation 10%
- HW Assignments 20%
- Lecture/video participation 5%

**14. Grading Scale**

Grading scale for the course: ≥90 A, ≥87 A-, ≥80 B, ≥77 B-, ≥ 70 C,≥ 67 C-,≥ 60 D, ≥ 57 D-,<57 F

**15. Make-up Exam Policy**

For the pass/fail evaluation of each module, students are allowed two tardy passes where a tardy is any module checked-off after the initial scheduled time. The tardy extension can be up to one week only and if a student falls too far behind they will be strongly encouraged to drop the class. After the first two free tardy extensions are used, additional tardy extensions result in a partial grade penalty – i.e. A=>A-…C-=>D+, one grade lower automatically per unsanctioned tardy.

**16. Honesty Policy**

All students admitted to the University of Florida have signed a statement of academic honesty committing themselves to be honest in all academic work and understanding that failure to comply with this commitment will result in disciplinary action. This statement is a reminder to uphold your obligation as a UF student and to be honest in all work submitted and exams taken in this course and all others.

**17. Accommodation for Students with Disabilities**

Students requesting classroom accommodation must first register with the Dean of Students Office. That office will provide the student with documentation that he/she must provide to the course instructor when requesting accommodation.

**18. UF Counseling Services**

Resources are available on-campus for students having personal problems or lacking clear career and academic goals. The resources include:

University Counseling Center, 301 Peabody Hall, 392-1575, Personal and Career Counseling.

SHCC mental Health, Student Health Care Center, 392-1171, Personal and Counseling.

Center for Sexual Assault/Abuse Recovery and Education (CARE), Student Health Care Center, 392-1161, sexual assault counseling.

Career Resource Center, Reitz Union, 392-1601, career development assistance and counseling.

**19. 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.