Course Syllabus

Jump to Today ✎ Edit

Syllabus for
EEL4714/EEL5716 - Introduction to Hardware Security and Trust

Spring 2018

1. **Catalog Description**

Fundamentals of hardware security and trust for integrated circuits and systems, 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. **Instructor/coordinator: Dr. Mark Tehranipoor**

Office Location	MAE 226
Office Hours	Mon 2-3pm
Class Location	NEB 201
Telephone	352-392-2585
Email	tehranipoor@ece.ufl.edu (mailto:tehranipoor@ece.ufl.edu)
Website	http://tehranipoor.ece.ufl.edu (http://tehranipoor.ece.ufl.edu)

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

Adib Nahiyan, adib1991@ufl.edu (mailto:adib1991@ufl.edu) (Wed 3-4pm)

Andrew Stern, andrew.stern@ufl.edu (mailto:andrew.stern@ufl.edu) (Wed 3-4pm)

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	09	4:05-4:55PM
Thursday	08-09	3:00-4:55PM

7. **Meeting Location (for In-campus students) -** NEB 201
8. **Material and Supply Fees**
   Avnet Spartan-6 LX9 MicroBoard for each project team ($~100/team) – each team may include up to 3 students.
   (**https://www.xilinx.com/products/boards-and-kits/1-3i2dfk.html** (https://www.xilinx.com/products/boards-and-kits/1-3i2dfk.html))

9. **Textbooks and Software Required**

Textbook: None

Recommended Reference Book:

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

Software: Xilinx ISE package, Synopsys Verilog simulation package and HSpice, Cadence Design System, Programming and Scripting Software (Matlab, Python, C/C++)

10. **Recommended Reading and Videos**

Reading

- **Mihir Bellare and Phil Rogaway, Introduction to Modern Cryptography** (http://www-cse.ucsd.edu/users/mihir/cse207/classnotes.html)
- **Ross J. Anderson. Security Engineering: A guide to building dependable distributed systems. John Wiley and Sons, 2001** (http://www.cl.cam.ac.uk/~rja14/book.html)
- **Matt Bishop , Computer Security: Art and Science, Addison-Wesley, 2003** (http://nob.cs.ucdavis.edu/book/book-aands/index.html)
- **William Stallings. Cryptography and Network Security, Fourth edition, 2007** (http://williamstallings.com/Crypto/Crypto4e.html) (WS)
- **The Hunt for the Kill Switch** (http://spectrum.ieee.org/tag/hardware+Trojan)
- **Hardware Trojan (computing)** (http://en.wikipedia.org/wiki/Hardware_Trojan_(computing))
- **Defense Science Board Task Force On High Performance Microchip Supply** (http://www.acq.osd.mil/dsb/reports/2005-02-HPMS_Report_Final.pdf)
- **Old Trick Threatens the Newest Weapons** (http://www.nytimes.com/2009/10/27/science/27trojan.html?_r=2&emc=eta1)
- **A Survey of Hardware Trojan taxonomy and Detection** (http://www.computer.org/portal/web/csdl/doi/10.1109/MDT.2009.159)
- **Detecting malicious inclusions in secure hardware: Challenges and Solutions** (http://www.engr.uconn.edu/~tehrani/publications/host08_2.pdf)
- **FPGA Design Security Bibliography** (http://www.cl.cam.ac.uk/~sd410/fpgasec/)
- **Supergeek pulls off 'near impossible' crypto chip hack** (http://www.nzherald.co.nz/technology/news/article.cfm?c_id=5&objectid=10625082&pnum=0)
- **Security through obscurity** (http://en.wikipedia.org/wiki/Security_through_obscurity)
- **Trust-Hub** (http://www.trust-hub.org/)

Videos

- What's inside a microchip? **http://www.youtube.com/watch?v=GdqbLmdKgw4** (https://mail.engr.uconn.edu/owa/redir.aspx?C=RHkmL0GLwE6y55XRg-EetI90hfH8x9EILte2x7bwb2Kwv30Q8pCu5Lxp0PGJkUJiYS6ozkr5jeg.&URL=http%3a%2f%2fwww.youtube.com%2fwatch%3fv%3dGdqbLmdKgw4)
- Zoom Into a Microchip **http://www.youtube.com/watch?v=Fxv3JoS1uY8** (https://mail.engr.uconn.edu/owa/redir.aspx?C=RHkmL0GLwE6y55XRg-EetI90hfH8x9EILte2x7bwb2Kwv30Q8pCu5Lxp0PGJkUJiYS6ozkr5jeg.&URL=http%3a%2f%2fwww.youtube.com%2fwatch%3fv%3dFxv3JoS1uY8)
- Public Key Cryptography: RSA Encryption: **http://www.youtube.com/watch?v=wXB-V_Keiu8** (https://mail.engr.uconn.edu/owa/redir.aspx?C=RHkmL0GLwE6y55XRg-EetI90hfH8x9EILte2x7bwb2Kwv30Q8pCu5Lxp0PGJkUJiYS6ozkr5jeg.&URL=http%3a%2f%2fwww.youtube.com%2fwatch%3fv%3dwXB-V_Keiu8)
- Counterfeit Electronics Could Be Dangerous, Funding Nefarious People **http://www.youtube.com/watch?v=dbZiUe6guxc** (https://mail.engr.uconn.edu/owa/redir.aspx?C=73Jh2CMQRUmnMNWxKjWrQvqwsrG9z9ElpE1FMYscahzd9XrTZaJUbF7s0KAmzxUucj1OoCVvLC8.&URL=http%3a%2f%2fwww.youtube.com%2fwatch%3fv%
- How Computers and Electronics Are Recycled **http://www.youtube.com/watch?v=lw4g6H7alvo** (https://mail.engr.uconn.edu/owa/redir.aspx?C=73Jh2CMQRUmnMNWxKjWrQvqwsrG9z9ElpE1FMYscahzd9XrTZaJUbF7s0KAmzxUucj1OoCVvLC8.&URL=http%3a%2f%2fwww.youtube.com%2fwatch%3fv%
- Counterfeit Electronic Components Process **http://www.youtube.com/watch?v=5vN_7NJ4qYA** (https://mail.engr.uconn.edu/owa/redir.aspx?C=73Jh2CMQRUmnMNWxKjWrQvqwsrG9z9ElpE1FMYscahzd9XrTZaJUbF7s0KAmzxUucj1OoCVvLC8.&URL=http%3a%2f%2fwww.youtube.com%2fwatch%3fv%
- Counterfeit Inspection **http://www.youtube.com/watch?v=MbQUvu2LN6o** (https://mail.engr.uconn.edu/owa/redir.aspx?C=73Jh2CMQRUmnMNWxKjWrQvqwsrG9z9ElpE1FMYscahzd9XrTZaJUbF7s0KAmzxUucj1OoCVvLC8.&URL=http%3a%2f%2fwww.youtube.com%2fwatch%3fv%
- Gold from waste circuit electronics **http://www.youtube.com/watch?v=ZkhOuNvkuu8** (https://mail.engr.uconn.edu/owa/redir.aspx?C=73Jh2CMQRUmnMNWxKjWrQvqwsrG9z9ElpE1FMYscahzd9XrTZaJUbF7s0KAmzxUucj1OoCVvLC8.&URL=http%3a%2f%2fwww.youtube.com%2fwatch%3fv%
- Tarnovsky Deconstruct Processor **https://www.youtube.com/watch?v=w7PT0nrK2BE** (https://mail.engr.uconn.edu/owa/redir.aspx?C=1iGyFEKyhU-UFbB79afyqpQvr-SA69EIuE88wZr26-zos8uXDR1MTj8zV8soZW_dPBNMBKi4_Y8.&URL=https%3a%2f%2fwww.youtube.com%2fwatch%3fv%3dw7PT0nrK2BE)

11. **Course Outline**

Week	Tuesday Lecture	Instructor	Thursday Lecture	Instructor
Week 1 (Jan 9, 11)	Syllabus, Ethics, Introduction to hardware security and trust, Emerging applications and the new threats	MT	Introduction	MT
Week 2 (Jan 16, 18)	Introducing Thursday Activities + VHDL/Verilog & FPGA Tutorial	STA	Introduction to Cryptography	MT
Week 3 (Jan 23, 25)	VHDL/Verilog & FPGA Tutorial	STA	Basics of VLSI Design and Test	MT
Week 4 (Jan 30, Feb 1)	VHDL/Verilog & FPGA Tutorial	STA	Security Based on Physically Unclonability and Disorder	MT
Week 5 (Feb 6, 8)	VHDL/Verilog & FPGA Tutorial + Project Description	STA	Hardware Metering	MT
Week 6 (Feb 13, 15)	Student Presentations	MT/STA	Watermarking of HW IPs	MT
Week 7 (Feb 20, 22)	Student Presentations	MT/STA	Physical Attacks and Tamper Resistance	MT
Week 8 (Feb 27, Mar 1)	Student Presentations	MT/STA	Security in Embedded Systems + **Midterm**	MT
Week 9 (Feb 28, Mar 2)	Student Presentations	MT/STA	Fault Injection Attacks, Security of RFID Tags	MT
Week 10	SPRING BREAK			
Week 11 (Mar 13, 15)	Student Presentations	MT/STA	Protecting against Scan-based Side Channel Attacks	MT
Week 12 (Mar 20, 22)	Student Presentations	MT/STA	Basics of PCB Security	MT
Week 13 (Mar 27, 29)	Student Presentations	MT/STA	Hardware Trojans: IC Trust (Taxonomy and Detection)	MT
Week 14	Student	MT/STA	Counterfeit Detection	MT

(Apr 3, 5)	Presentations		and Avoidance	
Week 15 (Apr 10, 12)	Student Presentations	MT/STA	Hardware Trojans: IP Trust (Detection) + Design for Hardware Trust	MT
Week 15 (Apr 17, 19)	Student Presentations	MT/STA	Side Channel Attacks and Countermeasures, Countermeasures for Embedded Microcontrollers	MT
Week 16 (Apr 24)		MT	Reading day	

12. **Attendance and Expectations**

Format: The course is comprised of weekly lectures, 3-4 HW assignments, 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. It will be considered cheating and will be dealt with in a severe manner. See Section 16 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.

The EDGE students may complete the paper presentation and final project module individually or as a team of 3. A separate instruction set will be issued for individual paper presentations and projects.

13. **Grading-methods of evaluation**

- Exams 45% (20% mid-term, 25% final (comprehensive))
- HW Assignments 15%
- Final Project 20%
- Oral Paper Presentation 20%

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.

Course Summary:

Date	Details