ELEC 5210/6210 - HARDWARE SECURITY I

Catalog Data:

ELEC 5210 - HARDWARE SECURITY I (3) LEC. 3, Pr., ELEC 2200. Hardware design of symmetric and asymmetric ciphers, digital signature generation and verification, key management, detection and avoidance of counterfeit ICs, cryptographic primitives, and automated hardware design aids.

ELEC 6210 - HARDWARE SECURITY I (3) LEC. 3. Hardware design of symmetric and asymmetric ciphers, digital signature generation and verification, key management, detection and avoidance of counterfeit ICs, cryptographic primitives, and automated hardware design aids.

References Books*:*

1. *Understanding Cryptography: A Textbook for Students and Practitioners,* C. Paar, and Jan Pelz, Springer-Verlag Berlin Heidelberg, 2010, ISBN 978-3-642-04100-6
2. *Counterfeit Integrated Circuits: Detection and Avoidance*, M. M. Tehranipoor, U. Guin, and D. Forte, Springer International Publishing, 2015, ISBN: 978-3-319-11823-9

Coordinator: Ujjwal Guin, Assistant Professor of Electrical & Computer Engineering

Goals:

Secure electronic products play an important role in safeguarding our society and day-to-day lives. Many different electronic devices that are connected to the Internet, have exhibited an increasing level of heterogeneity in recent years. Maintaining security over all these different devices becomes extremely challenging, as they are being designed and manufactured in an environment with limited trust and visibility. Various new attacks are emerging to circumvent existing security measures. To enable secure and trustworthy operations, it is absolutely necessary to understand these attacks and incorporate appropriate security measures. This course is intended for the graduate and undergraduate students who are interested in designing secure systems. This course will provide an in-depth analysis of various topics, which include (i) introduction to cryptography - symmetric and asymmetric ciphers, message authentication codes, and digital signatures, (ii) detection & avoidance of counterfeit ICs, and (iii) security primitives - physically unclonable functions (PUFs) and true random number generators (TRNGs).

Outcomes:

By the end of this course,

1. The student will
   a. Demonstrate proficiencies in concepts, techniques, and applications of cryptography.
   b. Demonstrate proficiencies in hardware implementations of a popular crypto primitive.
   c. Demonstrate proficiencies in understanding hardware security issues.
   d. Demonstrate proficiencies in understanding hardware security primitives.
   e. Demonstrate proficiencies in applying cryptography and security primitives to address hardware security issues.
2. 6000-level students will
   f. Demonstrate critical thinking and analytical skills through a summary and evaluation of an open hardware security problem.

Prerequisites by topic: ELEC 2200 - Digital Logic Circuits

Weekly Topics:

1) Introduction to cryptography
2) Stream Ciphers
3) Data Encryption Standard (DES) (HW1 Due)
4) Advanced Encryption Standard (AES)
5) Introduction to VHDL/Verilog (HW2 Due)
6) Public Key Cryptography (Project P1 Due)
7) RSA Cryptosystem (Test 1)
8) Discrete Logarithm Problems (Project P2 Due)
9) Message Authentication Codes (HW3 Due)
10) Digital Signatures (Project P3 Due)
11) Semiconductor Supply Chain (HW4 Due)
12) Counterfeit Integrated Circuits (Project P4 Due)
13) Detection and Avoidance of Counterfeit ICs (Test 2)
14) Physically Unclonable Functions
15) True Random Number Generators (Project P5 Due)
16) FINAL EXAM (Presentation and Final report on Open Problem)

Methods for evaluating student performance:

	Undergraduate Students	Graduate Students
Homework	25%	20%
Class tests (2)	25%	20%
Design Project	25%	20%
Open Hardware Security Problem	---	20%
Final Examination	25%	20%
TOTAL	**100%**	**100%**

Grading Scale:

90-100	A
80-89	B
70-79	C
60-69	D
<60	F

Homework: Problems will be assigned throughout the semester to reinforce the class material. The homeworks are summarized as follows:

HW1: Modular arithmetic, basics of ciphers, and brute force effort computation.
HW2: One-time pad (OTP), pseudorandom number sequence generation using LFSR, stream cipher, and DES.
HW3: Galois Field, AES, and RSA.
HW4: Diffie-Hellman Key Exchange (DHKE), digital signature and Message Authentication Code (MAC).

Design Project: Advanced Encryption Standard (AES) crypto primitive with key size 128 will be designed in the VHDL modeling language, verified via Xilinx Vivado Design Suite, and a working implementation on a supplied FPGA board. The project will be due on the last class day. Parts of it will be assigned, collected, and graded throughout the semester. 80% of the project grade will be from these individual parts; the other 20% will be for the final project and simulation. Project grades will include components for correctness of design, modeling technique, testing, and documentation. The parts are summarized as follows:

P1: Overall architecture, design environment setup, and Sbox implementation
P2: Shift-row and mix-column implementation
P3: Key addition and one complete round implementation
P4: Complete AES simulation
P5: Hardware implementation and a working AES demo

Note that every group is expected to do their own project. Discussion of various aspects of the project with fellow groups is acceptable, provided that designs are not copied. Copying of another group's project will be considered a violation of the academic honesty code by both groups, and will be dealt with as outlined in the "Tiger Cub".

Open Problem in Hardware Security:
Each student will be assigned to an open problem in Hardware Security. Some of the problems are – detection and avoidance of counterfeit ICs, prevention of the piracy of intellectual properties, design of a stable PUF, compact design of a TRNG, etc. The students are required to understand the threat, the existing solutions, which partially address the threat, and then proposed a new solution (idea) to solve the problem. A final presentation and a report will be due at the last day of class.

Justification for Graduate Credit in ELEC 6210:

- Graduate students are challenged with an open hardware security problem. They need to perform a detailed background study and propose a solution. They also need to submit a report, which is similar to an IEEE conference paper.

Academic Honesty Policy: All portions of the Auburn University student academic honesty code (Title XII) found online at http://www.auburn.edu/academic/provost/academicHonesty.html apply to this class. Every student is expected to do his/her own homework and research. Discussion of various aspects with fellow students is acceptable, provided that they are not similar. Copying of another student's solution will be considered a violation of the academic honesty code by both students.

Class attendance: Class attendance is highly encouraged but will not be accounted for in the course grade.

Policy on unannounced quizzes: There will be no unannounced quizzes.

Accommodations: Any student requiring special accommodations should come by my office within the first two days of class, bringing your letter from the Office of Students with Disabilities, 1244 Haley Center, 844-2096 (V/TT).

Prepared by: Ujjwal Guin   Date: 08/18/2021