ELEC 5290/6290 – HARDWARE SECURITY II

Catalog Data:

ELEC 5290 - HARDWARE SECURITY II (3) LEC. 3, Pr., ELEC 5210. Hardware design of symmetric and asymmetric ciphers, elliptic curve cryptosystems, SHA-3, side-channel attacks, modeling and test generation for hardware Trojans, cryptographic primitives, RFID security, and blockchain.

ELEC 6290 - HARDWARE SECURITY II (3) LEC. 3. Hardware design of symmetric and asymmetric ciphers, elliptic curve cryptosystems, SHA-3, side-channel attacks, modeling and test generation for hardware Trojans, cryptographic primitives, RFID security, and blockchain.

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
3. *Mastering Bitcoin: Programming the Open Blockchain*, Andreas M. Antonopoulos, O'Reilly, 2017, ISBN-13: 978-1491954386

Coordinator:

Ujjwal Guin, Assistant Professor of Electrical & Computer Engineering

Goals:

Secure electronic products play an essential role in safeguarding our society and day-to-day lives. Many different electronic devices that are connected to the Internet have exhibited an increased level of heterogeneity in recent years. Maintaining security over all these different devices becomes exceptionally 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. It is essential to understand these attacks and incorporate appropriate security measures to enable secure and trustworthy operations. This course is intended for graduate and undergraduate students who are interested in designing secure systems. This course provides an in-depth analysis of various topics, including advanced cryptography, hardware Trojans, PUFs, RFID security, side-channel attacks and solutions, and blockchain.

Outcomes:

By the end of this course,

1. The students will
   a. Demonstrate proficiencies in concepts, techniques, and applications of cryptography.
   b. Demonstrate proficiencies in hardware implementations of different popular crypto primitives.
   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 5210/6210 - Hardware Security I

Weekly Topics:

1: Introduction
2: Block Ciphers: Modes of Operation
3-4: Elliptic Curve Cryptosystems (Project P1 Due)
5: Hash function: SHA-3 (HW1 Due)
6: Key Establishment
7: Side-Channel Analysis (HW2 Due)
8-9: Hardware Trojans (Test 1, and Project P1 Due)
10: Detection and Avoidance of Counterfeit Integrated Circuits
11-12: Physically Unclonable Functions (PUFs)
13: RFID Security (Project P3 Due)
14-15: Blockchain (Project P4 Due)
16: FINAL EXAM (Presentation and Final report on Open Problem)

Methods for evaluating student performance:

	Undergraduate Students	Graduate Students
Homework	20%	10%
Class Tests (1)	15%	10%
Design Project	40%	40%
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. Homeworks are summarized as follows:

HW1: Fundamental calculation related to elliptic curve cryptography (ECC), Double-and-Add algorithm, and ECC application in DHKE.
HW2: Key Freshness and Key Derivation, Key Establishment Using a Key Distribution Center, and Key exchange protocols.

Design Project: A secure cryptoprocessor will be designed in the VHDL/Verilog 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 the correctness of design, modeling technique, testing, and documentation. The parts are summarized as follows:

P1: Design and implementation of AES with Counter (CTR) Mode
P2: Design and implementation of RSA
P3: Design and implementation of a secure hash function (SHA-3)
P4: Complete cryptoprocessor Implementation in an FPGA

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, detection, and avoidance of tampering (unwanted modification), detection of cloned hardware, design of an efficient blockchain instance, 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 on the last day of class.

Justification for Graduate Credit in ELEC 6290:

- 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 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: 1/5/2021