ELEC 5970/ELEC 6970: HARDWARE SECURITY-I
Fall Semester, 2018, TUESDAY-THURSDAY, 11AM, BROUN 306

Catalog Data: ELEC 5970 SPECIAL TOPICS IN ELECTRICAL ENGINEERING (1-5) LEC. Course may be repeated with change in topics.

ELEC 6970/6976 SPECIAL TOPICS IN ELECTRICAL ENGINEERING (1-5) LEC. Departmental approval. Study of a specialized area of electrical and computer engineering not covered by regularly offered courses. Course may be repeated with change in topics. Course may be repeated for a maximum of 24 credit hours.

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. *Introduction to Hardware Security and Trust*, M. Tehranipoor, C. Wang, Springer-Verlag New York, 2012, ISBN 978-1-4419-8079-3

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 provides an in-depth analysis of various topics, which include introduction to cryptography, detection & avoidance of counterfeit ICs, security primitives, and side-channel attacks & solutions.

Prerequisites by topic: Not Applicable

Topics (with approximate distribution of lectures): 27 Classes

1. Introduction (1 class)
2. Introduction to cryptography (1 class)
3. Symmetric Ciphers (4 classes)
4. Asymmetric Ciphers (4 classes)
5. Message Authentication Codes (2 classes)
6. Digital Signatures (2 classes)
7. Key Management (2 classes)
8. Side-Channel Analysis (2 classes)
9. Semiconductor Supply Chain (1 class)
10. Counterfeit Integrated Circuits (1 class)
11. Detection of Counterfeit ICs (2 classes)
12. Avoidance of Counterfeit ICs (2 classes)
13. Physically Unclonable Functions (PUFs) (2 classes)
14. True Random Number Generators (TRNGs) (1 classes)

Methods for evaluating student performance:

Homework	25%
Class tests (2)	25%
Design Project	25%
Final Examination	25%
TOTAL	**100%**

Homework:

Problems will be assigned throughout the semester to reinforce the class material.

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.

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".

Justification for Graduate Credit in ELEC 6970:

Graduate students are challenged with a current security problem and are also expected to research and report their ideas to solve it.

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: 08/06/2018