ECE 4823A/8873A Advanced Hardware Oriented Security and Trust
Proposed Credits: **3 lecture hours per week = 3 credit hours total**

Prerequisites: ECE 3020 or ECE 3894 (HOST) or undergraduate ECE degree

Proposed course material:
(Books) Alfred Menezes, Paul van Oorschot and Scott Vanstone, Handbook of Applied Cryptography, 5th printing, CRC Press, 1996, and Jonathan Katz & Yehuda Lindel, Introduction to Modern Cryptography, CRC Press, 2015
(Lecture Notes) To be distributed via a course website

Course Syllabus and Topical Outline
Module 1: Advanced Authentication

- Message Authentication Codes (MAC)
- Entropy & randomness
- Multi-party authentication

Module 2: Modern Cryptography

- Data privacy
- Secret sharing
- VLSI design of cryptographic hardware
- AES, ECC and Keccak SHA

Module 3: Physically Uncloneable Functions (PUFs)

- PUF construction classes
- PUF entropy sources
- PUF metrics & attacks including machine learning
- Practical considerations including current status

Module 4: Hardware and Software Vulnerabilities

- Common weakness enumerations
- Secure boot
- Timing Attacks
- Countermeasures in hardware

Module 5: Hardware Attacks

- Hardware Trojans (HTs)
- Reverse engineering

Evaluation Criteria: The course will have two midterm exams, a final exam and frequent homeworks/labs. Labs will be based on VHDL and associated digital design (e.g., Synopsys Design Compiler) and simulation tools. This class may be taught in one section with both graduate students as well as undergraduates; to distinguish course expectations, graduate students will have to answer an additional question on an advanced topic on homeworks and exams. For example, for an exam with five questions, the instructions will indicate that the fifth question is more advanced and should only be answered by students enrolled in the graduate section of the course.