Proposed Undergraduate Course Title: **Hardware Oriented Security and Trust**
Proposed Credits: **3 lecture hours + 3 lab hours per week = 4 credit hours total**

Prerequisites: ECE 2040, ECE 3020 and ECE 2031

Proposed course material:
(Books) Jonathan Katz & Yehuda Lindel, Introduction to Modern Cryptography, CRC Press, 2015, and Tehranipoor et al., Introduction to Hardware Security and Trust, Springer, 2012
(Lecture Notes) To be distributed via a course website

Course Syllabus and Topical Outline
Module 1: Authentication
- Access control, challenge-response, keys
- Entropy & randomness, one-way functions
- VLSI circuits and characteristics

Module 2: Cryptography from a hardware-centric perspective
- Data privacy, integrity and authenticity
- Historic ciphers: substitution, permutation/transposition and one-time pads
- Symmetric and asymmetric keys, models and protocols
- VLSI design of cryptographic hardware
- AES, ECC and Keccak SHA

Module 3: Power Analysis Attacks
- Simple Power Analysis
- Differential Power Analysis
- Electro-Magnetic (EM) Analysis

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: Cryptographic Hardware and Vulnerabilities
- ASIC versus FPGA versus Microprocessor (i.e., software)
- Side Channel Analysis
- Timing Attacks
- Countermeasures in hardware

Module 5: VLSI Test, Supply Chain and Hardware Attacks
- Design verification and manufacturing test
- Hardware Trojans (HTs)
- Relationship between physical faults (test) and malicious attack (HTs)

Evaluation Criteria: The course will have two midterm exams, a final exam and frequent homeworks/labs (typically each week except the week of an exam). Labs will be based on VHDL and associated digital design and simulation tools (e.g., ModelSim).