Instructor: **Assoc. Prof. Vincent J. Mooney III**
Course Number: **ECE 3170 A / LA** (Section A is for the lecture while Section LA is for the lab credit)
Course Title: **Cryptographic Hardware for Embedded Systems**
Course Credits: **3 lecture hours + 3 lab hours per week = 4 credit hours total**

Prerequisites: ECE 2040 and ECE 2031

Course material:
(Book) Bruce Schneier. Applied Cryptography, John Wiley & Sons, 1996
(Lecture Notes) To be distributed via a course website

Course Syllabus and Topical Outline
Module 1: Authentication

- Access control, challenge-response, keys
- One-way functions
- VLSI circuits and characteristics

Module 2: Cryptography from a hardware-centric perspective

- Data integrity and authenticity
- Historic ciphers: substitution, permutation/transposition and one-time pads
- Symmetric and asymmetric keys, models and protocols
- DES and associated cryptographic hardware

Module 3: Power Analysis Attacks

- Simple Power Analysis
- Differential Power Analysis
- Electro-Magnetic (EM) Analysis

Module 4: Cryptographic Hardware and Vulnerabilities

- ASIC versus FPGA versus Microprocessor (i.e., software)
- Side Channel Analysis

Module 5: VLSI Test, Supply Chain and Hardware Attacks

- Design verification and manufacturing test
- Relationship between physical faults (test) and malicious attack (Hardware Trojans)

Evaluation Criteria: The course will have two midterm exams, a final exam and frequent homeworks/labs (typically one homework is due each week except for approximately five weeks which have both a homework and a lab due). Labs will be based on VHDL, associated digital design and simulation tools (e.g., ModelSim) and an FPGA board donated by Intel for this course. The percentage of the final grade for each component is 15% for homeworks, 20% for labs, 15% for each midterm and 35% for the final (please note that in future semesters these percentages may vary but will always add up to 100%). The initial typical grading curve of 90% and above is an A, 80-89% B, 70-79% C, 60-69% D and below 60% is an F will be modified to remain or become more lenient after each exam. For example, after the first midterm exam the curve could be moved to 89% and above is an A, 80-88% B, 70-79% C, 58-69% D and below 58% is an F. Once moved, the curve will never move back up, e.g., if a B is moved to be 79-88% is a B then the curve will never go back up to 80-89% is a B.

Mode of Instruction for Fall 2025: The course will be taught in person with reasonable effort made to also provide lectures live on-line (synchronous) as well as recorded for later viewing (asynchronous). However, the on-line and recorded options are not guaranteed to always be available (100% of the time). In order to make time in class to go over homework questions, some (approximately 25%) of the lectures maybe be prerecorded while the rest of the lectures will be provided live in person, i.e., during the posted class meeting times in the official classroom. Class time will also be used to go over practice problems, e.g., old exams, to help prepare for the midterms and the final. For classes delivered live in the classroom while simultaneously broadcasting (e.g., using Zoom or Teams) and recording the lectures, typically a recording of each synchronous class (regardless of content, i.e., including both lecture material as well as problem solving sessions) will be made available in the Media Gallery on Canvas within 24 hours after each class. Typically Kaltura Capture is used to record class, but broadcast software (e.g., Zoom or Teams) may also be used. Due to ongoing concerns about viruses and other forms of communicable diseases, it is anticipated that not all students will want to attend all classes live in person. Therefore, other than for exams and to pick up the hardware (an FPGA board and a ChipWhisperer board) to be loaned out for labs, in-person class attendance will not be required for this class, but it will be highly encouraged subject to health considerations. Class attendance will be required for all exams (midterms and the final); remote taking of exams will not be provided. Any medical or other emergency situation is covered by Attendance & Absences below.

Learning Objectives: As a part of this course, students perform the following:

1. Apply knowledge of mathematics and computing to understand cryptography and authentication.
2. Master core concepts of cryptographic hardware design.
3. Obtain laboratory experience in protection, analysis and side-channels of cryptographic digital logic.
4. Learn modern automatic VLSI synthesis, simulation and analysis tools using state-of-the-art facilities.
5. Apply the engineering design process to design cryptographic hardware that meets the constraints of time, cost, energy and security.

Learning Outcomes: Upon successful completion of this course, students will be able to do the following:

1. Analyze the level of security provided by symmetric encryption algorithms such as DES and asymmetric encryption algorithms such as RSA.
2. Write VHSIC Hardware Description Language (VHDL) code to implement encryption algorithms including synthesis to hardware logic gates.
3. Provide approaches to authentication able to resist attacks such as man-in-the-middle and replay.
4. Explain dangers associated with hardware Trojan insertion of logic gates in the chip design process including the manufacturing supply chain.

5. Make tradeoffs between execution speed, area, energy/power and resistance to side-channel analysis and attacks for practical digital logic implementations of encryption and authentication.

Attendance & Absences: Students with medical, family or other critical emergencies should contact the Office of the Dean of Students. Students should familiarize themselves with http://www.catalog.gatech.edu/rules/4/. To the extent possible, students should communicate excused absences in advance; when not possible, students shall communicate their excused absences as soon after the emergency as can reasonably be expected for the situation. Late assignments will not be accepted for credit without an excused absence. Missed exams will be handled on a case-by-case basis typically in close coordination and cooperation with the Office of the Dean of Students.

As noted above under Mode of Instruction, in-person class attendance is only required for exams and to pick up the hardware boards used for labs. The aim is to provide the majority of lectures in a remote fashion duplicating (albeit imperfectly) the classroom instruction. However, please note that while 100% reliable internet cannot be guaranteed, Kaltura Capture runs locally and records all class material regardless of periodic internet connectivity problems. In other words, subject to software and/or hardware problems (such as a microphone malfunction), all class content will be available and uploaded for students to view after the fact. Students who choose to attend remotely and miss portions of class due to internet connectivity and other similar issues are responsible for viewing the lecture recording of any material missed. Students are responsible for all class content.

Honor Code: Students are expected to hold the highest ethical standards not only for this class but for the rest of their professional careers. Hardware security is a very serious topic and is critical to ensuring privacy, confidentiality and a healthy society. However, ethics in this course start and end in the human person. The Georgia Tech Honor http://www.policylibrary.gatech.edu/student-affairs/academic-honor-code Code http://catalog.gatech.edu/rules/18/ holds in all of its parts. When there is reasonably clear evidence of a violation, a referral to the Office of the Dean of Students will occur, and all hearings and other resulting procedures will be followed to completion.

Office of Disability Services: Students who are registered with the Office of Disability Services (ODS) shall provide appropriate forms and paperwork in person to the course instructor. If you think you may have learning needs, feel free to contact the Office of Disability Services at (404) 894-2563 or https://disabilityservices.gatech.edu/. An accommodation letter must be obtained from ODS in order to receive accommodations.