Introduction to the Course
ECE 4156/6156 Hardware-Oriented Security and Trust

Spring 2024

Assoc. Prof. Vincent John Mooney III

Georgia Institute of Technology

Topics

- Advanced Authentication
  - Message Authentication Code (MAC) design
  - Multi-party authentication
- Modern Cryptography
  - Advanced Encryption Standard (AES)
  - Secret sharing
- Physically difficult for yoU to clone Functions (PUFs)
- Secure Boot
- Timing attacks
- Hardware Trojans

Course Organization

- Lecture T/Th 2:00pm-3:15pm (tentative, not yet finalized!)
  - Aim to broadcast all lectures with Zoom and record with Kaltura Capture
    - Please only use the first initial of your last name in Zoom, e.g., “George B.”
    - Note1: Kaltura Capture records locally, so if there are network issues please review the lecture recording which will be uploaded within 24 hours of completion of each class
    - Note2: this class is not provided immediate support for audio or video issues; still responsible for all class content
- Grading policy
  - Homeworks 15%
  - Midterm I 15%
  - Labs 20%
  - Midterm II 15%
  - Final Exam 35%
- Website will contain lecture notes, homeworks, labs and other info
  - http://mooney.gatech.edu/Courses/ECE4156

Required Textbooks

Katz and Lindell, **Introduction to Modern Cryptography**, third edition, CRC Press, 2015, ISBN 9781466570269

Alfred Menezes, Paul van Oorschot and Scott Vanstone, **Handbook of Applied Cryptography**, 5th printing, CRC Press, 1996, ISBN 9781119096726

Optional Textbooks

Roel Maes, **Physically Unclonable Functions**, *Constructions, Properties and Applications*, Springer, 2013, ISBN 9783642413957

Bruce Schneier, **Applied Cryptography**, Second Edition, Wiley, 1996, ISBN 9781119096726

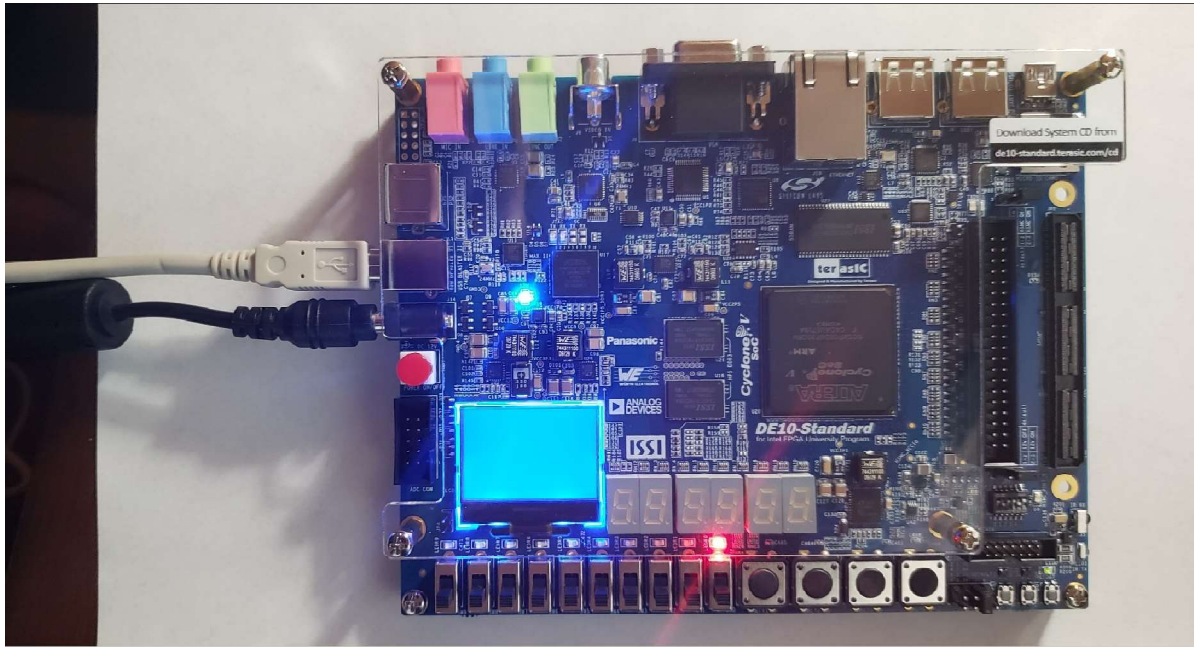
Stefan Mangard, Elisabeth Oswald and Thomas Popp, **Power Analysis Attacks**, *Revealing the Secrets of Smart Cards*, Springer, 2007, ISBN 9780387308579

Some comments regarding the books

- The Georgia Tech Library has an agreement with Springer, so while you are a student you may obtain from Springer a pdf file of most of their textbooks, including **Physically Unclonable Functions** and **Power Analysis Attacks**, and you may keep electronic copies of such textbooks on your computer up and until you graduate
- Once purchased, you may share the required textbooks among friends (e.g., if several of you are taking this course together)

Labs

- Intel DE-10 Standard FPGA board with ARM processor
- Recent donation
- Labs from previous years implement cryptographic algorithms in VHDL and C/C++



- This year will be the same except that the teaching assistant will port all of the labs to this new board
- You may use a board in Klaus 1446/8 or may sign one out to take home

Prerequisites

- Undergraduate degree

  - OR –

- ECE 3020 Mathematics of Computer Engineering

  - OR –

- ECE 3057/8 Architecture, Systems, Concurrency and Energy in Computation

  - OR –

- ECE 3170 Cryptographic Hardware for Embedded Systems

Canvas

- Grades
- Announcements
- Class recordings in the Media Gallery
- Homework and lab submissions

Office Hours

- Check out course web page
  - http://mooney.gatech.edu/Courses/ECE4156
- Look under “General Information”
  - http://mooney.gatech.edu/Courses/ECE4156/info.html
  - Professor office hours TBD
    - These hours are designed to provide an opportunity for everyone
- TA office hours will be posted specific to lab assignments
  - Availability of additional TA hours will depend on enrollment

Exams

- There are three exams – two midterms and a final – for this course
- Remote taking of exams is not supported; you must come to campus
- All exams will be in class and taken on paper
  - Exams will be open book and notes

Suggested Strategy

- Start homeworks and labs early, e.g., try to answer the first question right away
- If stuck, try to formulate two options which have nonidentical results and both of which appear reasonable to you; then ask how to resolve
- Will accept any and all homework and lab questions at the beginning of each class only; together with office hours MW, there are four days a week prescheduled for you to ask questions!!!
- If there are a lot of questions early and late, may extend due dates for entire class
- In answering questions, may give away part of the answer & will provide this to the entire class

Academic Integrity

- Where is “the line” in doing assignments?
- DO:
  - Talk about the course concepts with your classmates
  - Discuss the homework concepts with your classmates to clarify conceptual misunderstandings
- DO NOT:
  - Work “together” to solve an assignment
  - Turn in identical papers
  - “Share” any computer code (including both C/C++ and VHDL) or other lab executable (e.g., a bitstream)
- ANY VIOLATION WILL BE REFERRED TO THE DEAN OF STUDENTS

Plagiarism

- Merriam-Webster defines plagiarism as “the act of using another person's words or ideas without giving credit to that person”
- You may not quote any lectures word for word to answer a homework or exam question
- You may not quote a homework solution to answer an exam question (you will be allowed to write information on a sheet of paper for each exam – I recommend you do not put quotes of others on the sheet, including from lectures or homeworks)

GT Honor Code

- http://www.honor.gatech.edu/
- Academic misconduct includes but need not be limited to the following:
  - Possessing, using or exchanging improperly acquired written or verbal information in the preparation of any essay, laboratory report, examination, or other assignment included in an academic course;
  - Substitution for, or unauthorized collaboration with, a Student in the commission of academic requirements;
  - Submission of material that is wholly or substantially identical to that created or published by another person or person, without adequate credit notations indicating authorship (plagiarism);
  - False claims of performance or work that has been submitted by the claimant;
  - Alteration or insertion of any academic grade or rating so as to obtain unearned academic credit;
  - Deliberate falsification of a written or verbal statement of fact to a member of the Faculty so as to obtain unearned academic credit;
  - Forgery, alteration or misuse of any Institute document relating to the academic status of the Student.

Questions?