Introduction to the Course

Cryptographic Hardware for Embedded Systems

ECE 3170 A

Fall 2024

Assoc. Prof. Vincent John Mooney III

Georgia Institute of Technology

Introduction

- Logic design
  - Very Large Scale Integration (VLSI) digital circuits
  - System-on-a-Chip (SoC)
    - Microprocessors (software)
    - Reconfigurable logic
    - Custom logic
- Cryptography
  - Security of communications
  - Trust of sources and authorship
  - Mathematical basis and relationship to hardware (logic) design

Topics

- Cryptography
- Authentication
- Cryptographic hardware
- Algorithmic attacks
- Power analysis attacks
- Digitals systems test
- Supply chain attacks

Course Organization

- Lecture T/Th 2:00pm-3:15pm
  - 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.”
    - Note Kaltura Capture records locally, so if there are network issues please review the lecture recording if available (aim to upload within 24 hours of completion of each class)
  - Whitaker 1103
- Grading policy
  - Homeworks 15%
  - 1st Midterm 15% – likely at the end of September, but the exact date will be determined a 2-3 weeks prior
  - Labs 20%
  - 2nd Midterm 15% – likely in November, exact date to be determined
  - Final Exam 35%
- Website will contain lecture notes, homeworks, labs and other info
  - http://mooney.gatech.edu/Courses/ECE3170

Exams

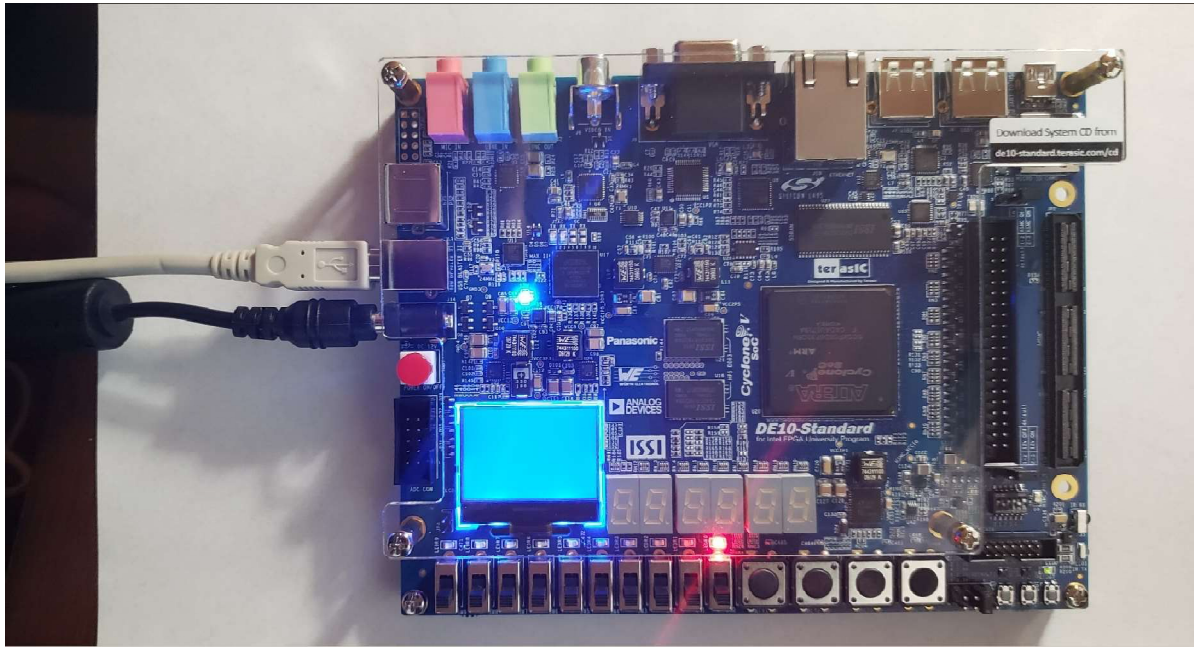
- There are three exams – two midterms and a final – for this course
- Remote taking of exams is not supported; you must come to campus
- All exams will be in class, Whitaker 1103, on paper
  - Exams will be open book and notes; details to be provided closer to the first exam, e.g., not all books will be allowed to avoid students bringing a library…
- In general, graded exams will not be returned electronically; you must come to campus to pick up your exam in person (typically in class or office hours)

Required Textbook

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

Labs

- Intel DE10 Standard FPGA board with ARM processor
- Recent donation
- Labs from previous years implement cryptographic algorithms in VHDL and C/C++



- This is the second year that we will be using this board; the teaching assistant will be rewriting most of the labs to improve them
- You must sign one out and may use it in Klaus 1446/8 or at home

Prerequisites

- ECE 2031 and ECE 2040

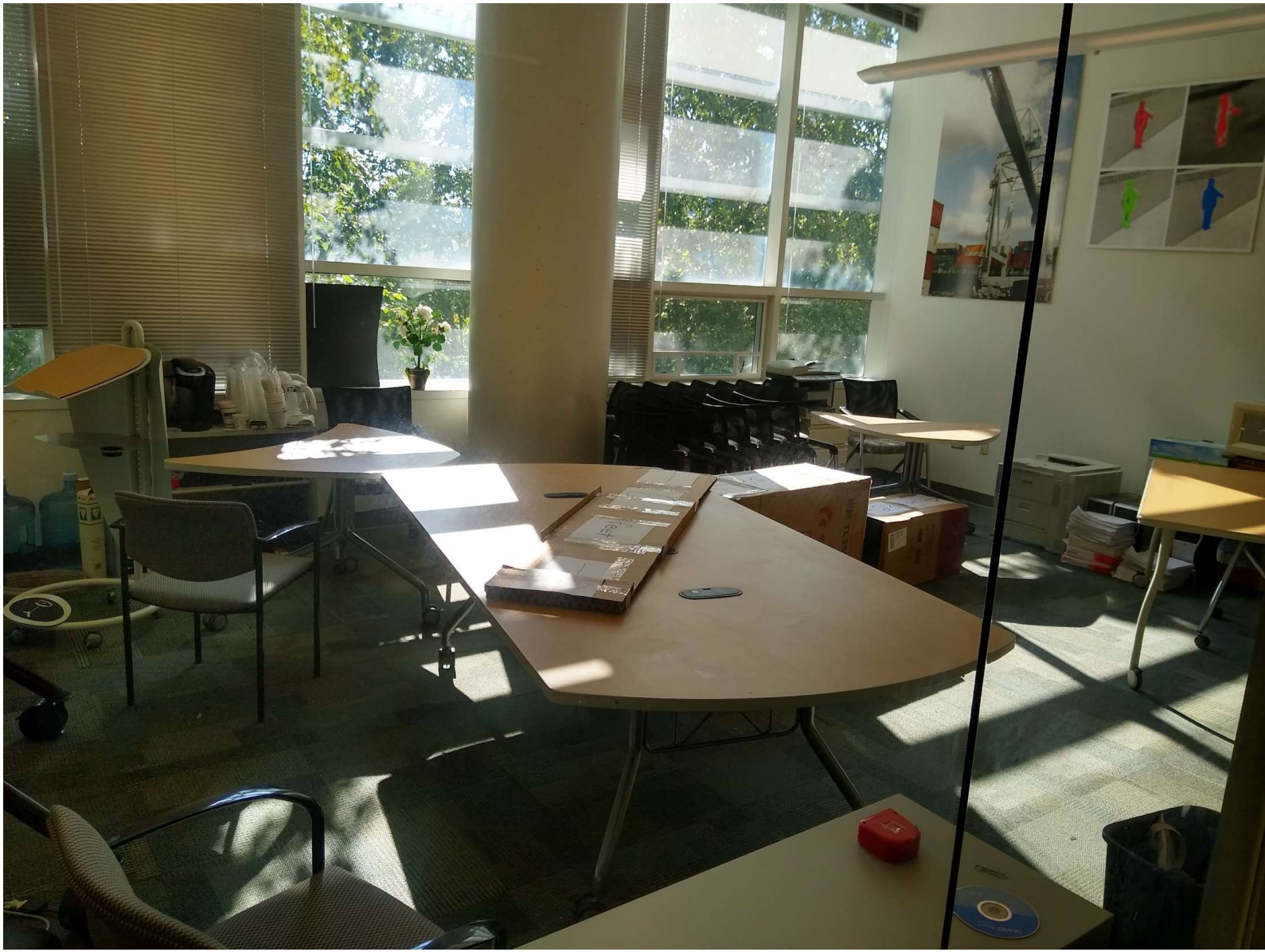
Canvas

- Announcements
- Media Gallery
- Homework and laboratory submissions
  - Grades for these submissions
- Piazza

Office Hours

- See website for posted office hours; may change based on student feedback!
- Keep track of announcements for any last minute changes
- Aim to support both in-person and remote students simultaneously (except for exams which will be in-person only!)
- Generally allow all technical questions to be heard by everyone
- May request assistance in making recordings for interesting topics

Klaus 2350 (view from hallway) office hours have plenty of space!



Academic Integrity

- Please refer to slide deck on this topic