

ECE 3170 Cryptographic Hardware for Embedded Systems

Fall 2025

Assoc. Prof. Vincent John Mooney III

Georgia Institute of Technology

Homework 12, 50 pts.

Due Friday Nov. 14 prior to 11:55pm

(please turn in homework electronically on Canvas)

As always this semester, you are required to solve any and all homework questions alone.

- 1) (10) Briefly describe the difference between detecting Trojans in hardware description language IP, e.g., in a VHDL module, and detecting them in a GDS II layout. What types of detection techniques can be used for each?
- 2) (10) Of the two types of Hardware Trojans described in the previous question, which one is more likely to be used by an adversary when the hardware platform is an FPGA? Why?
- 3) (10) Briefly describe one strategy that may be effective in distinguishing between a random manufacturing defect and a Hardware Trojan.
- 4) (20) Hardware Trojans can be classified into two basic classes, functionally disruptive and information leakage types. Indicate the basic detection strategies that are applicable for detecting Hardware Trojans in each class: detection strategies include logic testing, parametric testing and IC deprocessing.
 - a. (10) Functionally Disruptive: indicate the basic detection strategies that are applicable to detecting functionally disruptive Hardware Trojans and explain why.
 - b. (10) Information Leakage: indicate the basic detection strategies that are applicable to detecting information leakage Hardware Trojans and explain why.

YOU MAY NOT CONSULT HOMEWORK SOLUTIONS OF THESE EXACT PROBLEMS FROM OTHER COURSES. ALL LABORATORY SUBMISSIONS MUST INCLUDE YOUR NAME, COURSE NUMBER, SECTION, AND THE HOMEWORK SET NUMBER. ALL SHEETS MUST BE STAPLED TOGETHER. ALL WRITING MUST BE EASY TO READ (FOR EXAMPLE, YOU MAY HAVE TO WRITE ONLY ON ONE SIDE OF EACH SHEET OF PAPER THAT YOU SUBMIT AND MAY NOT BE ABLE TO USE RECYCLED PAPER). FAILURE TO FOLLOW INSTRUCTIONS MAY RESULT IN ZERO POINTS. ALL WORK MUST BE YOUR OWN. NO PLAGIARISM IS ALLOWED, AND YOU MUST PROPERLY REFERENCE ALL SOURCES OF YOUR INFORMATION – ALTHOUGH YOU SHOULD NOT LOOK FOR AND MAY NOT CONSULT “SOLUTIONS” AVAILABLE FROM OTHER SOURCES (TO REPEAT, YOU MAY NOT CONSULT HOMEWORK SOLUTIONS OF THESE EXACT PROBLEMS FROM OTHER COURSES!).