Hardware-Oriented Security and Trust
ECE 4156 A / ECE 6156 A
Spring 2026

Assoc. Prof. Vincent John Mooney III
Georgia Institute of Technology

Homework 10, 50 pts. (ECE 4156) 60 pts. (ECE 6156)
Due Friday April 17 prior to 11:55pm

1) (10 pts.) What is the purpose of a fuzzy extractor?

2) (20 pts.) Consider the reverse fuzzy extractor.
   a. (10 pts.) What is the purpose of a reverse fuzzy extractor? Be sure to distinguish your answer from the answer you gave for the purpose of a fuzzy extractor (see question 4 above); in other words, if you give the same answer here you will receive zero points.

   b. (10 pts.) What must the server do to the stored response bitstring it has in its secure database in a reverse fuzzy extractor scheme?

3) (10 pts.) Briefly describe the difference between detecting Hardware Trojans in a hardware description, e.g., a VHDL module, versus detecting Hardware Trojans in a GDS II layout. What types of detection techniques can be used for each?

4) (10 pts.) 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 Trojans in each class: detection strategies include logic testing, parametric testing and IC deprocessing.

   a. (5 pts.) Indicate the basic detection strategies for functionally disruptive Hardware Trojans.

   b. (5 pts.) Indicate the basic detection strategies for information leakage Hardware Trojans.

5) [ECE 6156 only!] (10 pts.) Why is it a concern in a reverse fuzzy extractor that the helper data changes from one run of the protocol to the next?

YOU MAY NOT CONSULT HOMEWORK SOLUTIONS OF THESE EXACT PROBLEMS FROM OTHER COURSES, INCLUDING OTHER/PREVIOUS SECTIONS OF ECE COURSES TAUGHT BY PROFESSOR MOONEY SUCH AS THOSE WITH NAMES INCLUDING HARDWARE ORIENTED SECURITY AND TRUST AS WELL AS CRYPTOGRAPHIC HARDWARE FOR EMBEDDED SYSTEMS. ALL HOMEWORK SUBMISSIONS MUST INCLUDE YOUR NAME, COURSE NUMBER, SECTION, AND THE HOMEWORK SET NUMBER. ALL SUBMISSIONS MUST BE DONE ONLINE. ALL WRITING MUST BE EASY TO READ (FOR EXAMPLE, YOU MAY HAVE TO WRITE WITH THICK INK AND MAY NOT BE ABLE TO USE LOW RESOLUTION PHOTOS OF HANDWRITTEN DIAGRAMS). FAILURE TO PROVIDE CLEAR AND LEGIBLE ANSWERS 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!).