Hardware-Oriented Security and Trust
ECE 4156 HST / ECE 6156 HST
Spring 2024

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

Homework 8, 75 pts. (ECE 4156) 80 pts. (ECE 6156)
Due Friday April 5 prior to 11:55pm

1) (15 pts.) For each of the following PUFs, use a few (e.g., between one and three) sentences to describe the source of entropy (randomness). Make sure to discuss both the physical as well as the functional aspects. (Note1: by physical what is meant are sources based in physical properties of materials and associated structures.) (Note2: by functional what is meant are sources due to logic design, e.g., Exclusive-OR logic functionality.)
   a. (5 pts.) Arbiter PUF
   b. (5 pts.) Ring Oscillator PUF
   c. (5 pts.) Metal Resistance PUF

2) (25 pts.) Consider the bit sequence 0 1 0 1 1 1 1 0 0 1 1 1 1 0 0 1 0 1 0 0 and apply the following tests. For each test, please show your work regarding how you calculated the numerical result; provision of only a numerical answer without showing the steps and calculations used will result in zero credit.
   a. (5 pts.) Entropy
   b. (5 pts.) MinEntropy
   c. (15 pts.) Conditional MinEntropy using pairs of two bits:
      0 1 0 1 1 1 1 0 0 1 1 1 1 0 0 1 0 1 0 0

3) (5 pts.) What defines an intrinsic PUF?

4) (10 pts.) Use your own words (do **not** copy from the lecture notes or any other source!) to answer the following question: what is the difference between a weak PUF and a strong PUF?

5) (10 pts.) Why are PUFs used for encryption not threatened by model building?

6) (10 pts.) Consider the tamper-evidence property of a PUF.
   a. (5 pts.) What is the tamper-evidence property? Please describe the tamper-evidence property of a PUF using your own words.
   b. (5 pts.) What does the tamper-evidence property of PUFs protect against?

7) [ECE 6156 only!] (5 pts.) Explain why a compressed file has more entropy than the same file uncompressed.

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!).