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

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

Homework 9, 110 pts. (ECE 4156) 135 pts. (ECE 6156)
Due Friday April 11 prior to 11:55pm

1) (40 pts.) Consider an instance of the HELP PUF with 2^{23} hazard-free paths. Assume that these hazard-free paths consist of 2^{22} rising (zero to one transition) paths and 2^{22} falling (one to zero transition) paths.

   a. (5 pts.) Describe the physical sources of entropy (randomness) in the HELP PUF.

   b. (10 pts.) Consider two specific paths whose delays are compared to produce a response bit. Discuss the entropy (i) on each path and (ii) in the comparison bit result. In particular, consider two PUF instances $HELP_1$ and $HELP_2$. Consider the same two specific paths in each HELP instance. Discuss the entropy in these paths for both $HELP_1$ and $HELP_2$.

   c. (10 pts.) Continuing in the previous question, discuss how the entropy on each path can change the comparison bit result. In particular, consider how the path lengths in $HELP_1$ and $HELP_2$ may be related (correlated) to each other due to the use of Hardware Description Language (HDL) synthesis tools.

   d. (15 pts.) Is it possible to build a model of the HELP PUF? In particular, assuming **you** are the adversary and **you** have access to the HELP PUF for a month, how would you propose to model build the HELP PUF? Make sure to discuss in your answer the fact that the HELP PUF you are trying to clone uses 2^{22} rising (zero to one transition) paths and 2^{22} falling (one to zero transition) paths.

2) (15 pts.) Consider a PUF which is enrolled and then tested a week later at all possible combinations of 0ºC, 25ºC, 85ºC and supply voltage (nominal), supply voltage (5% more than nominal) and supply voltage (5% less than nominal). Consider the case of a specific challenge-response pair. One approach to measure HD_{intra} is to compare the value of the response from enrollment versus the response from each of the combinations (nine comparisons total). A second approach is to compare each response with each other (45 comparisons in total). In your opinion, which approach is more appropriate for the authentication use case for the PUF (explain why)? Which approach to measure HD_{intra} is more appropriate for encryption (please explain why)?

3) (15 pts.) Are transistor delays a good source of randomness? Please explain (i) at least one reason why you think this is true and (ii) at least one reason why you think that this is not true.

4) (10 pts.) What is the purpose of a fuzzy extractor?

5) (10 pts.) What is the primary benefit of using a controlled PUF in a PUF-based authentication protocol?

6) (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?

7) [ECE 6156 only!] (15 pts.) How does TVcomp in HELP greatly reduce the variations in PND for the same challenges over a wide range of temperature and voltage conditions?

8) [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!).