# ECE 4156/6156

## Hardware-Oriented Security and Trust

# Midterm II

**April 18, 2024**

*This test is open book for the required as well as the optional textbooks. This test is also open note. Calculators are permitted but no programs may be used. Open notes include electronic notes with any handwritten or typed information you may have added. For electronic notes, all wireless connectivity must be turned off, and cell phones are not allowed; in other words, no connection to any information source outside of the open books, open notes and the course website is allowed during the exam. Open notes also include all course assignments (homeworks or labs) as well as solutions (including both your solution as well as official solutions posted on the course website or passed out for previous exams). All aspects of the Georgia Tech Honor Code apply. Please follow the instructions precisely. If you need to continue a problem, please use the back of the* ***previous*** *page. The meaning of each question should be clear, but please state any assumptions and ask for clarification if necessary.*

**You can do it!**

Name (Please print)___________________________________

This test will be conducted according to the Georgia Tech Honor Code. I pledge to neither give nor receive unauthorized assistance on this exam and to abide by all provisions of the Honor Code.

Signed___________________________________

| Question | Score | Max |
|---|---|---|
| 1 | | **15** |
| 2 | | **20** |
| 3 | | **10** |
| 4 | | **5** |
| 5 | | **5** |
| 6 | | **5** |
| 7 | | **20** |
| **Total** | | **60 or 80** |

1. **(15 pts.) Entropy Tests.**

Consider the bit sequence 1111010010110010. To repeat these 16 bits in groups of eight, the bit sequence is the following: 11110100 10110010. Please apply the following three tests. For each test, you are required to 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) (5 pts.) Conditional MinEntropy using pairs of two bits: 11 11 01 00 10 11 00 10

2. **(20 pts.) A New PUF Needs Testing.**

Your company has just come up with a novel implementation for a PUF in silicon and wants to see if the PUF will produce good results.

(a) (10 pts.) Your manager tells you to try to implement and simulate the novel PUF implementation in a simulator, e.g., ModelSim. Would the simulation software provide you with accurate results in order to properly judge the performance of the PUF, e.g., $HD_{inter}$ and $HD_{intra}$ values? For full credit, you must give at least one valid reason (and no invalid reasons) for your answer. You may indicate reason(s) you do not want graded by crossing the reason(s) out – in this case of crossing some of your answer out please circle what you want graded. A correct answer with no valid reason given will earn zero points. Please limit your answer to 10 sentences or less.

(b) (10 pts.) Continuing with issues regarding testing the novel PUF idea, you decide to synthesize the VHDL for your PUF using an appropriate synthesis tool for implementation in an FPGA. Your workflow consists of synthesizing a PUF bitstream, loading the bitstream onto the FPGA, and performing statistical testing on the output of your PUF. Before each test you resynthesize the PUF bitstream and you alter the VHDL slightly, e.g., you are editing your VHDL for a variety of reasons including trying out different language constructs which have the same meaning (e.g., case statements versus nested if-then-elses). Will this workflow provide you with accurate results about the performance of your PUF? For full credit you must give at least one valid reason (and no invalid reasons) for your answer. You may indicate reasons you do not want graded by crossing them out (in this case please circle what you want graded). A correct answer with no valid reason given will earn zero points. Please limit your answer to 10 sentences or less.

3. **(10 pts.) Arbiter PUF.**

You are given an Arbiter PUF composed of *n* switchboxes.

The Arbiter PUF has $2^n$ distinct possible challenge inputs. Suppose *n* is small enough that we can test the Arbiter PUF with all $2^n$ challenges and store the responses. Now consider that you run the NIST Test Suite (specifically, the responses are long enough to run all 15 tests) on the Arbiter PUF. Do you expect that the result will be that all or nearly all of the 15 tests will be passed? Why or why not? You must provide at least one valid reason for your answer to receive any points on this problem.

4. **(5 pts.) Physical Sources of Entropy.**

Please name at least **three** distinct possible physical sources of entropy which a PUF may utilize to provide PUF responses to challenges. If you name more than three, please indicate which three you want to be graded as your answer; if you give four or more and do not clearly indicate which three you want graded, you will lose points if any of your answers is incorrect. Finally, please note that a logical entity, e.g., a pipeline stage or a microprocessor instruction, is not a physical object.

5. **(5 pts.) Strong PUFs are Possible in Silicon.**

In the context of an intrinsic PUF implemented in Silicon, argue for the claim that it **is** possible to design a strong PUF on a single Silicon chip. For full credit, limit your answer to 10 sentences or less and give at least one valid technical reason for your answer. Please note that there are a variety of reasonable arguments that can be made; you only need to provide one solid reason to receive full credit.

6. **(5 pts.) Strong PUFs are Not Possible in Silicon.**

In the context of an intrinsic PUF implemented in Silicon, argue for the claim that it is **not** possible to design a strong PUF on a single Silicon chip. For full credit, limit your answer to 10 sentences or less and give at least one valid technical reason for your answer. Please note that there are a variety of reasonable arguments that can be made; you only need to provide one solid reason to receive full credit.

7. **[ECE 6156 only!] (20 pts.) Randomness, Entropy, PUFs and NIST Tests.**

One of the PUF designs described in detail this semester was HELP. At a research conference where HELP was discussed, the “processing steps” applied to the response bits was described as “increasing the entropy of the challenge-response space” of HELP.

(a) (10 pts.) Argue **in favor** of the claim that “processing steps” applied to the response bits results in “increasing the entropy of the challenge-response space” of HELP. You must provide at least one plausible argument with sufficient technical detail for your answer to receive any points on this problem. Please also note that if you make statements which are unambiguously incorrect or false, you will lose points for such statements even if you have other parts of your answer which are correct; therefore, if you do not want certain statements graded, you may want to cross them out.

(b) (10 pts.) Now argue **against** the claim that “processing steps” applied to the response bits results in “increasing the entropy of the challenge-response space” of HELP. You must provide at least one plausible argument with sufficient technical detail for your answer to receive any points on this problem. Please also note that if you make statements which are unambiguously incorrect or false, you will lose points for such statements even if you have other parts of your answer which are correct; therefore, if you do not want certain statements graded, you may want to cross them out.

**THIS IS THE LAST PAGE OF THE EXAM!**