ECE 4156/6156

Hardware-Oriented Security and Trust

Midterm II

April 20, 2023

*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!

Question	Score	Max
1		**20**
2		**30**
3		**30**
4		**20**
Total		**80 or 100**

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_____

1. **(20 pts.) Choice of PUF for Authentication.**

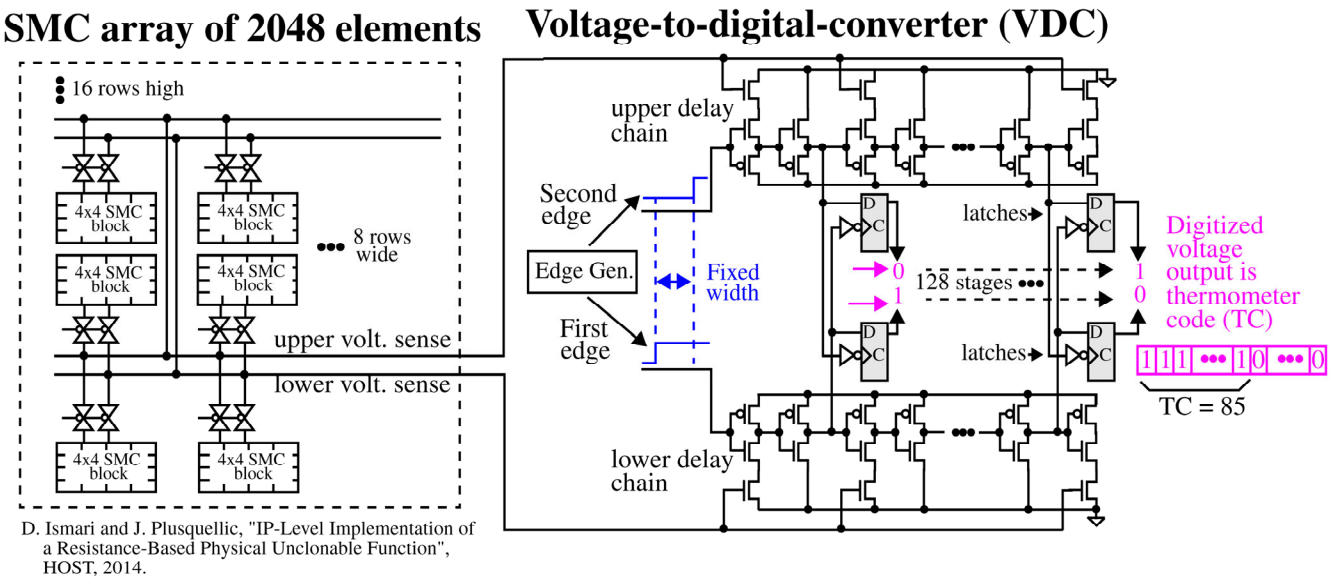
Consider a company that is designing an authentication system for an embedded system to be used in the field (e.g., a scooter or other IoT device which costs tens of thousands of dollars per scooter or device). The plan is for the IoT device (e.g., scooter) to implement a PUF for generating unique secret keys to authenticate each user (device) in the field (i.e., during use, e.g., two scooters may communicate directly with each other for real-time data collection). The company has four options for implementing the PUF: HELP, SRAM, Arbiter, or Ring Oscillator.

(a) (10 pts.) In this first scenario, the company's main concern is to minimize the cost of the PUF implementation while maintaining reasonable security. Which PUF should the company choose and why? Please provide at least one important and valid reason for your choice and no invalid or false reasons. Your answer should be limited to 10 sentences or less.

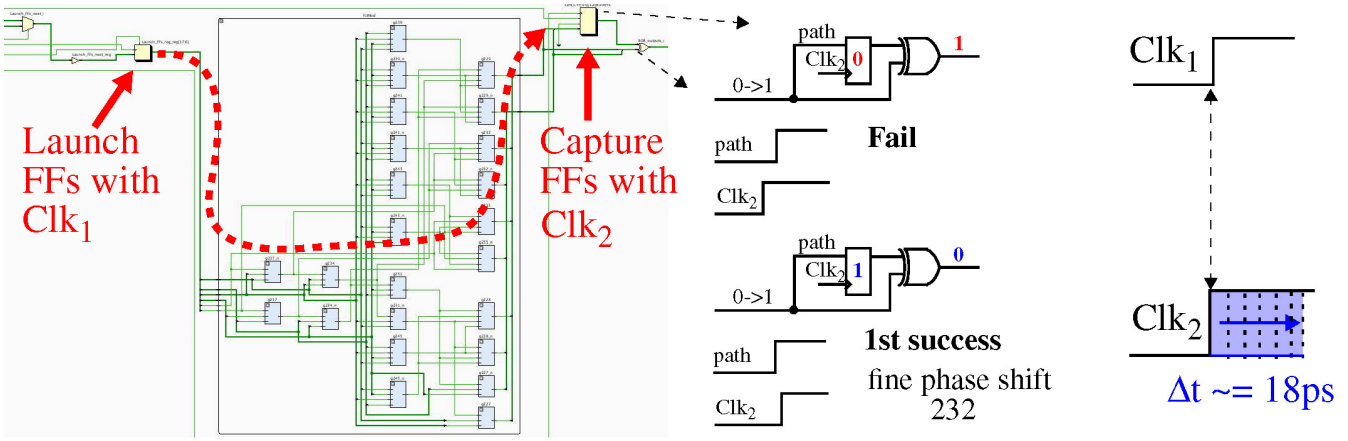
(b) (10 pts.) In this second scenario, the company's main concern is to maximize the security of the authentication system, even if it means higher costs for the PUF implementation. Which PUF should the company choose and why? Please provide at least one important and valid reason for your choice and no invalid or false reasons. Your answer should be limited to 10 sentences or less.

2. **(30 pts.) Measuring PUF Delays.**

One of the critical issues with PUFs is the measurement of variable delays. The ability to explain at a high level (i.e., an abstract level without all of the specific technology details) the mechanisms involved is important in evaluating the overall PUF. Part (a) asks about the Metal Delay PUF, and part (b) asks about HELP.



(a) (15 pts.) Explain in the above example how the thermometer code (TC) of 85 is found. Include in your explanation a discussion of (i) the upper versus lower voltage sense, (ii) edge generation including the first versus the second edge, (iii) the upper versus lower delay chain and (iv) the latches from which the final thermometer code (TC) is determined. NOTE1: you may answer with up to 10 sentences; if you give more than ten sentences, you must circle the sentences you want graded for your answer; if you give more than ten sentences without clearly indicating your answer, you will receive zero points. NOTE2: in your answer be sure to include a discussion of (i), (ii), (iii) and (iv) listed above or else you will lose points.



(b) (15 pts.) Explain in the above example how the PUF number of 232 is found. Include in your explanation a discussion of (i) "launch" Clk_1 versus "capture" Clk_2, (ii) the "fail" cases, and (iii) the "1st success" case. NOTE: you may answer with up to 10 sentences; if you give more than ten sentences, you must circle the sentences you want graded for your answer; if you give more than ten sentences without clearly indicating your answer, you will receive zero points.

3. **(30 pts.) Number of Physical Sources of Entropy.**

Consider the case of a chip design with ten billion transistors. Let us assume that the delay of each transistor can be individually measured and compared with any other transistor delay. You decide to use these delays to construct a PUF.

(a) (10 pts.) You decide to partition the transistors into two sets each with size 5 billion. You will compare only the following: a delay from the first set versus a delay from the second set. **How many comparisons** can you make with this PUF technique? (Ignore the cost of comparing in terms of transistor usage; assume that the comparisons can all be done for free.) NOTE: you must give a final numeric answer for full credit, i.e., a formula even composed of numbers (e.g., $7 * 10^3 * 7 * 10^3$) will lose points. (Of course, a number multiplied by a power is fine, e.g., $4.9 * 10^7$ is a perfectly valid answer.) HINT: pick one transistor from each set, measure delays for free, and compare; this is one comparison; continue in this manner for all possible comparisons.

(b) (10 pts.) Assuming that all ten billion transistors have delays whose variations are truly random, does the approach in part (a) result in a strong PUF? Assume that the adversary has the chip for a month (i.e., 30 days) and that one challenge-response pair per nanosecond (i.e., 10^{-9} seconds) can be calculated and stored by the adversary. You must give valid reasons to receive any credit for your answer to this question.

(c) (10 pts.) Now suppose that instead of comparing 5 billion delays with a different set of 5 billion delays, two delays are chosen from the full set of 10 billion delays. Would this change your answer to whether or not this is a strong PUF? Please note that a yes or no answer without valid reasons will earn zero points.

4. **[ECE 6156 only!] (20 pts.) Measurement Entropy.**

Both of the measurement techniques of thermometer code and fine phase shifting are likely to contribute some amount of entropy or randomness due to the measurement technique itself.

(a) (10 pts.) Considering extra entropy or randomness contributed by the measurement technique used in a particular PUF implementation, is this extra randomness in the measurement helpful or harmful in terms of $\mathbf{HD_{intra}}$? If the extra entropy is neutral, you may argue for neutrality as well (in addition to the question as stated, i.e., helpful versus harmful). For full credit, please explain at least one way in which HD_{intra} is most helped (or most harmed) by measurement entropy and clearly explain at least one valid reason why (and do not give invalid reasons!). Please circle the 10 sentences you want graded if you write down more than 10 sentences in your answer; equations or math do not count towards this 10-sentence limit.

NOTE: It is very likely that multiple answers will be accepted for this question; what is most important is that you give valid reasons for your answer!

(b) (10 pts.) Considering extra entropy or randomness contributed by the measurement technique used in a particular PUF implementation, is this extra randomness in the measurement helpful or harmful in terms of $\mathbf{HD_{inter}}$? If the extra entropy is neutral, you may argue for neutrality as well (in addition to the question as stated, i.e., helpful versus harmful). For full credit, please explain at least one way in which HD_{inter} is most helped (or most harmed) by measurement entropy and clearly explain at least one valid reason why (and do not give invalid reasons!). Please circle the 10 sentences you want graded if you write down more than 10 sentences in your answer; equations or math do not count towards this 10-sentence limit.

NOTE: It is very likely that multiple answers will be accepted for this question; what is most important is that you give valid reasons for your answer!

THIS IS THE LAST PAGE OF THE EXAM!