ECE 525 HOST: Midterm Exam

Name:

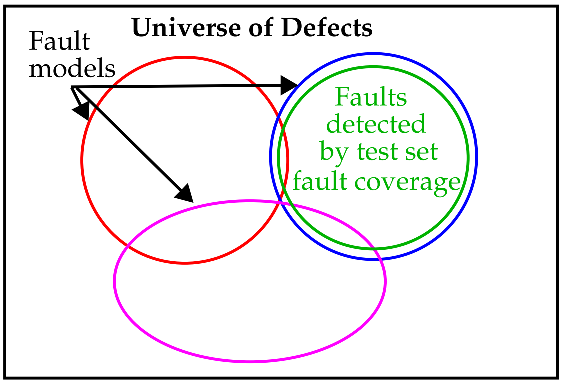
This exam is 5 pages long and has 10 questions + 1 Extra credit question

You must show all of your work -- partial credit may be given to partially correct answers, while answers with no justification may not receive full points. Use the back of the exam sheets if you need extra space.

1) (10 pts) Name (do not describe) 5 different focus areas of hardware-oriented security and trust.

2) (10 pts) Briefly describe (3 sentences max) the main differences between an FPGA flow and an ASIC flow.

3) (10 pts) How are physical defects different from a faults? Use the following diagram to explain your distinction(s).



4) (10 pts) Name three 'types' of modifications an adversary can make to the GDS II of an IC, i.e., what types of effects can these modifications have?

5) (10 pts) Name one advantage that can be leveraged in the testing process when we can assume that, if a Trojan exists, it will exist in EVERY chip.

6) (10 pts) Describe three basic approaches that have been proposed for detecting Trojans, and identify one advantage that each approach has over the other two.

7) (10 pts) Briefly explain the three quality metrics that are applied to PUF bit streams and how they can be measured using software techniques.

8) (10 pts) The arbiter PUF can generate an exponential number of response bits, 2^n, using an n bit challenge where a RO PUF can only generate n^2 response bits. However, the arbiter PUF is no 'stronger' than the RO PUF from an attack perspective (actually, it may be in fact weaker). Why?

9) (10 pts) Why do I claim that the Power Grid PUF is a 3-dimensional PUF, as opposed to all other PUFs which are 2-dimensional?

10) (10 pts) Briefly describe the three general applications of PUFs, and the importance of each on doing well on the metrics you described in Question 7.

Extra credit) (10 pts) Briefly describe the caveat of using soft information, i.e., magnitude of the difference between two delays, and a 'threshold' method to avoid error correction in secret key **re**-generation.