*EEL4720 Final Project Report*

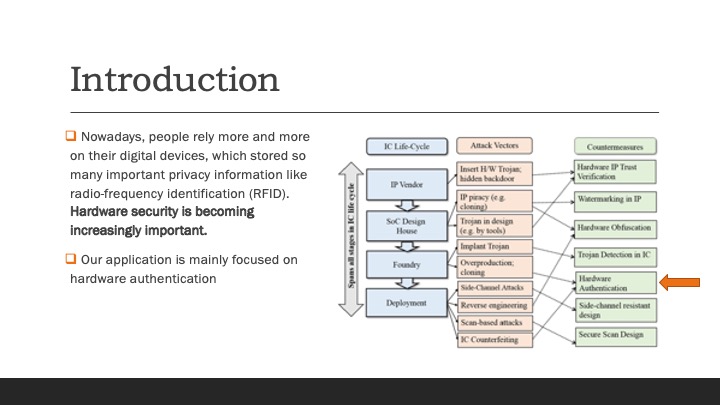
*(Note: the annotations are in blue and italic to make them more distinguishable from the slide text.)*

**

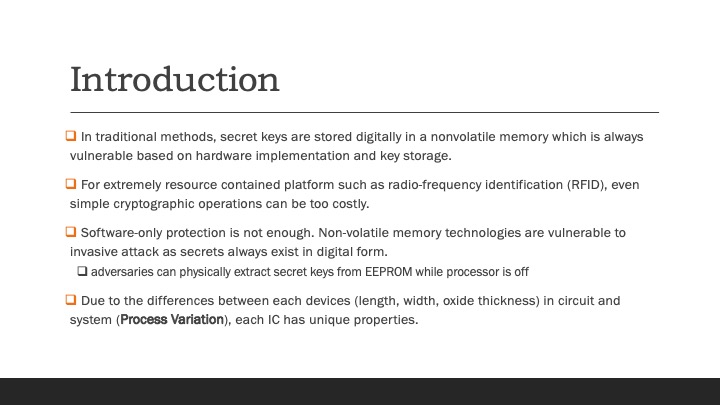
*A picture containing bird

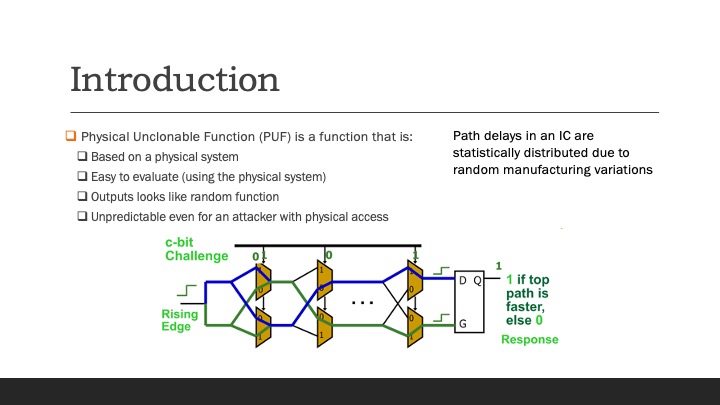
Description automatically generated*

*We discussed first five topics during progress report. We found a way to partially solve the problem afterwards, which was mainly discussed in final meeting.*

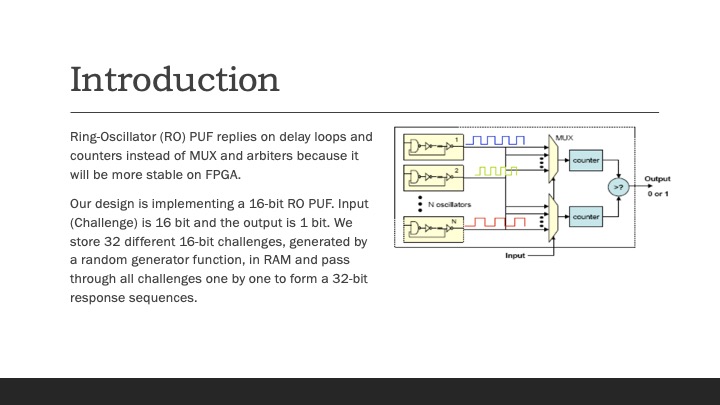
**

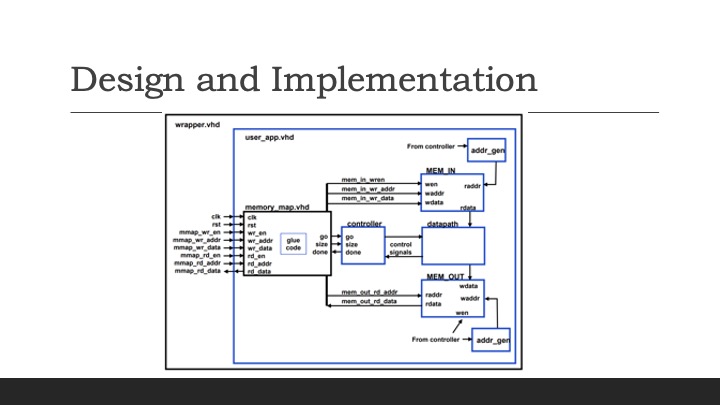
*In the whole process of IC lifecycle, there are a lot of potential attack vectors exist along with its countermeasures. Our application is mainly focus on Hardware Authentication*

**

**

*This is the structure of the basic physical unclonable function, what we designed are shown below.*

**

**

*The user\_app design is basically same as our lab 5, the only differences will be the data path, which is shown below. Later in the report, we will show how we are testing for this design. There are 25\*32\*6 = 4800 challenges input, so we need to use RAM to store the input and output.*

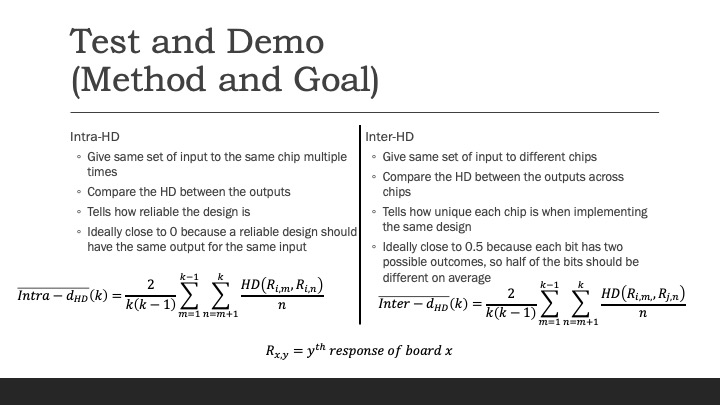
*A screenshot of a cell phone

Description automatically generated*

*Our design includes 256 ring oscillators, each path includes 30 not gates and a nand gate. The outputs of ring oscillator connect to two MUX, each of them takes an 8-bit input. The output of the MUX will be connected to the counters to calculate the times the output becomes 1. After certain time period, which is controlled by timer, the comparator will compare the results from two counters. The output will be 1 if counter1 larger than counter2, 0 otherwise.*

*A screenshot of a cell phone

Description automatically generated*

**

*To see how our design performs, we evaluate two criteria. The intra-HD tells how reliable our design is, so it should ideally be zero. The inter-HD tells how unique each FPGA is when implementing our design, so it should be close to 0.5.*

*A screenshot of a cell phone

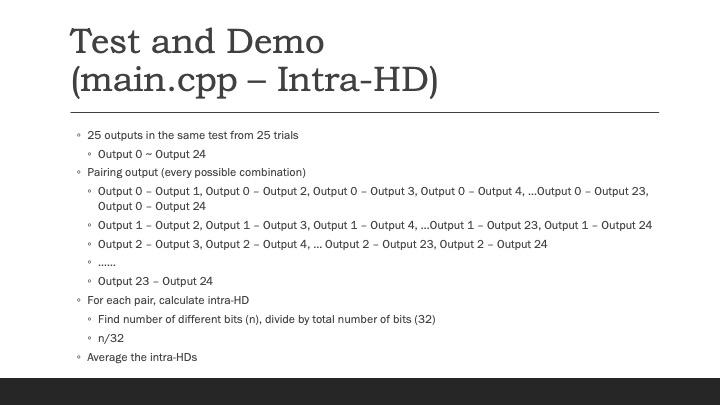
Description automatically generated*

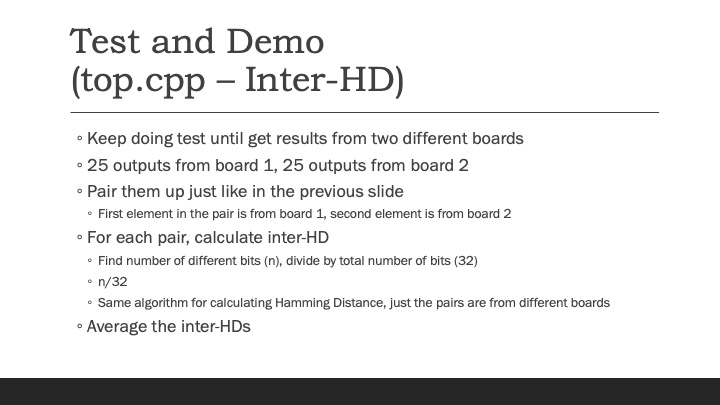
*Because we need data from two different boards to calculate inter-HD, I used a top.cpp program to help run the code on the FPGA and process the output data from different boards.*

*A screenshot of a cell phone

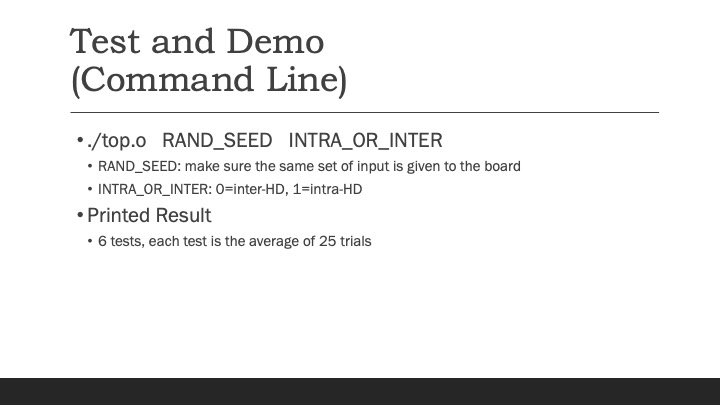
Description automatically generated*

*Since each challenge produces one 1-bit output, we group 32 challenges together to produce a 32-bit output. We have 6x32=192 challenges, so we can produce 6 different 32-bit outputs. This test is performed 25 times so that we can get the average value for inter-HD and intra-HD.*

**

**

*These two slides show how the outputs are paired when calculating the hamming distances.*

**

*This is how we use the terminal to run our test.*

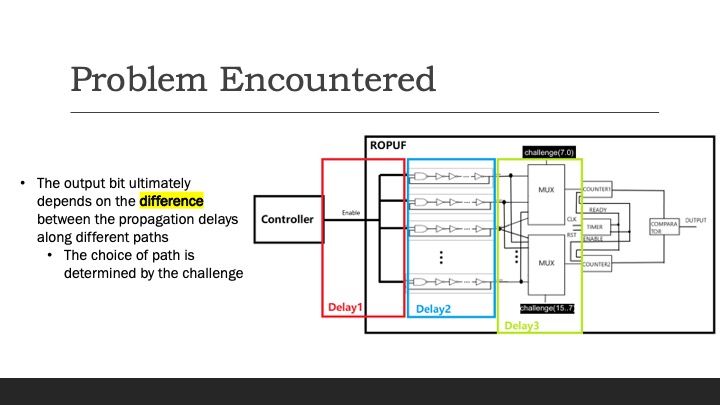
*Note: when RAND\_SEED=0, I use time(NULL) as the seed, so it will be complete random.*

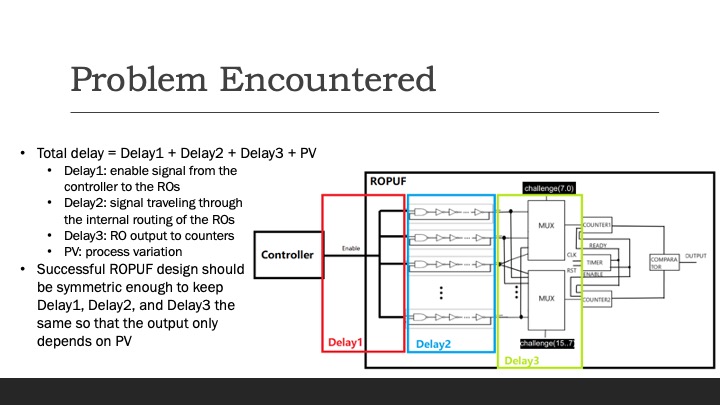
*A screenshot of a cell phone

Description automatically generatedA screenshot of a cell phone

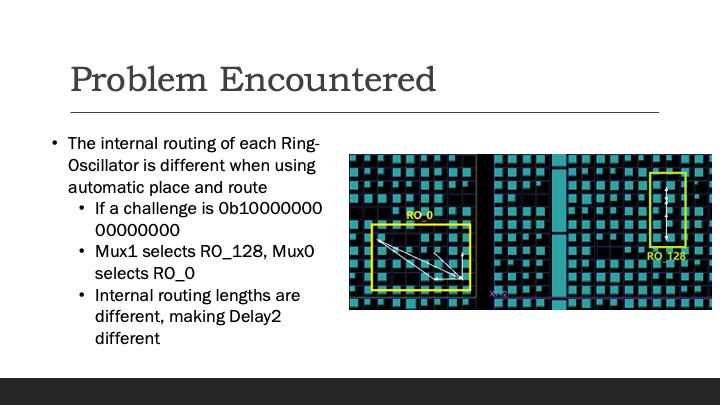
Description automatically generated*

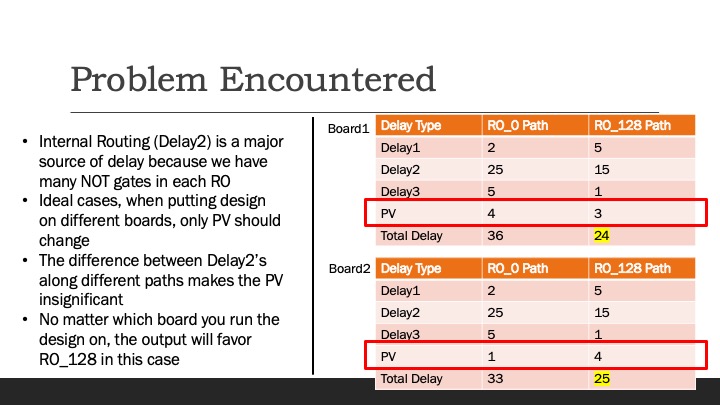
*These are our initial testing results. The intra-HD is very good, so our design is reliable. However, the inter-HD is far from 0.5, so our design does not reflect the uniqueness of each FPGA.*

**

**

*The output ultimately depends on the difference between the delays when the signal goes through different paths. In a successful ROPUF design, PV should be the only factor that affect the output, so the paths from the controller to the 256 ROs (Delay1) should be identical, the paths inside each RO (Delay2) should be identical, and the paths from the ROs’ outputs to the counters (Delay3) should be identical.*

**

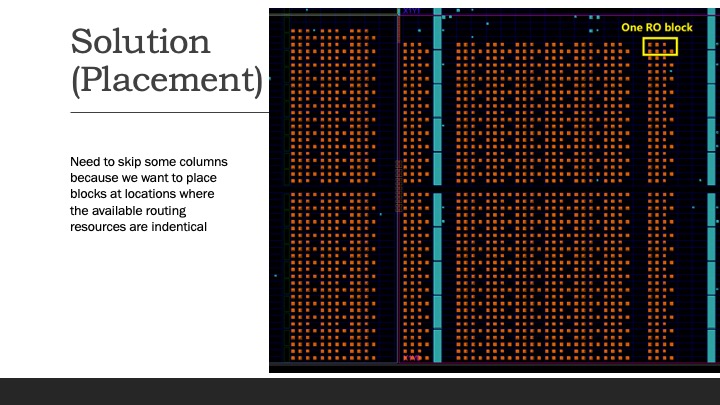
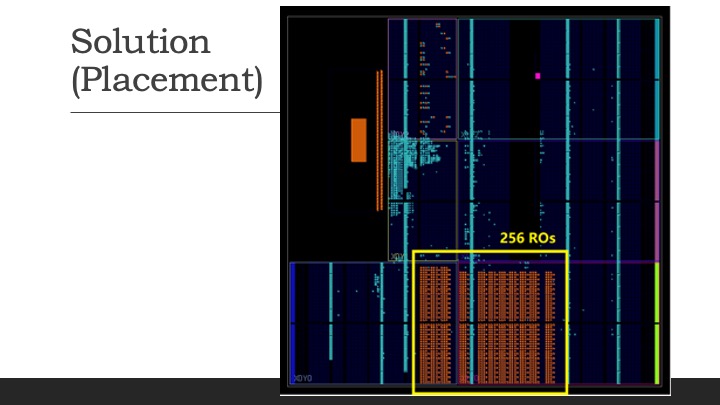
**

*The table on the right side is used to be an example, to explain why symmetric designs are so important, and the data were made up rather than extracted. The process variation will be hard to measure since that is the feature of the physical devices.*

*A screenshot of a cell phone

Description automatically generated*

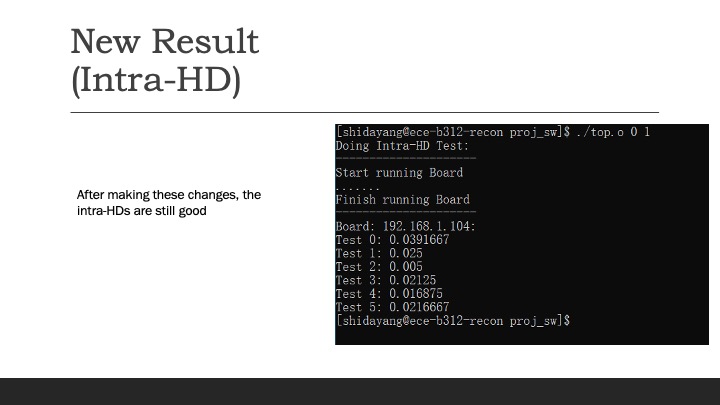
*Note: I will attach how I did this in another file (place\_and\_route\_using\_tcl\_commands.pdf)*

**

*This shows the placement of the LUTs of the ROs.*

*A screenshot of a cell phone

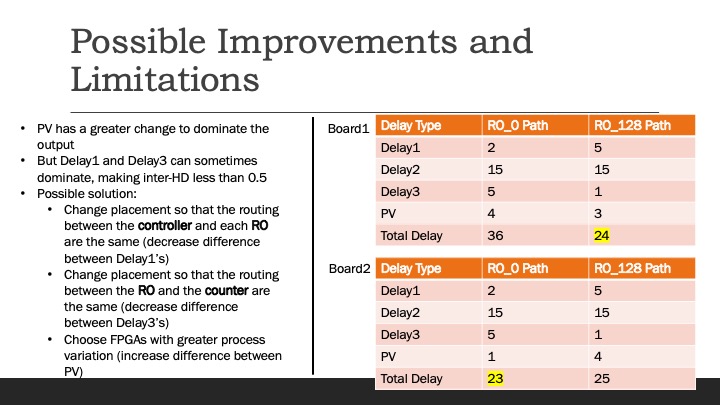
Description automatically generated*

*We had to skip some columns to find identical routing resources.*

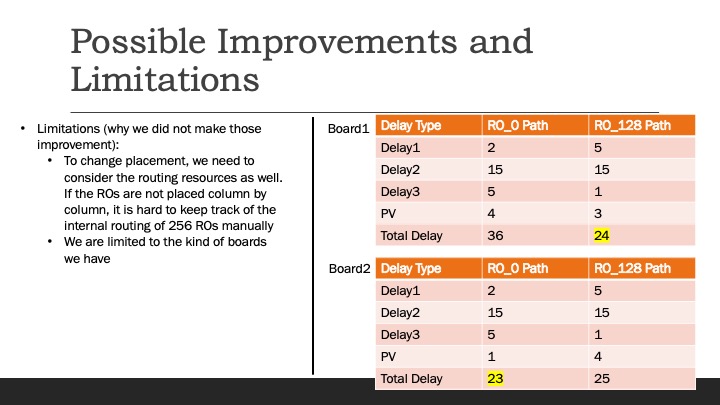
*After changing our design, the inter-HD is still good.*

**

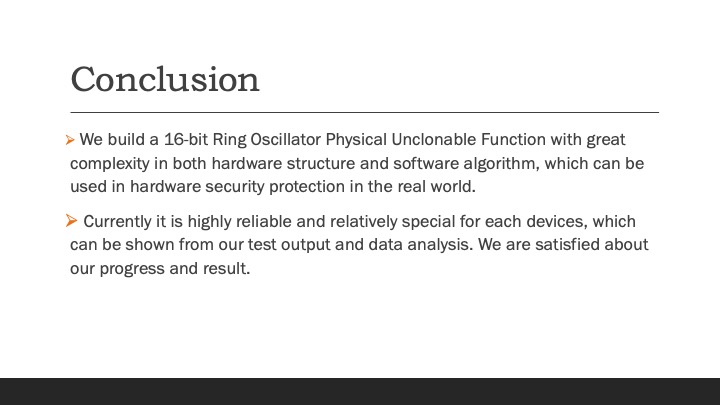
*We also see a significant improvement in the inter-HD. However, it is still not perfect.*

**

*The reason is that our change only solved the problem for Delay2, but Delay1 and Delay3 are still different. Even though PV has a greater change to dominate now, Delay1 and Delay3 may also dominate sometimes. The solution is to change the placement of our design to make all the Delay1’s identical and all the Delay3’s identical. Or, we can also find FPGAs with greater PV.*

**

*The solutions are not feasible at this point given the reasons in the slide.*

**

*Our design is highly reliable, but it does not show the uniqueness of each FPGA perfectly. However, we identified the issue and partially solved it after doing some research. Even though our design is not perfect, it is still useable in real world. Since the difference between the inter-HD and the intra-HD is significant enough, we can easily set a threshold (like 0.05) to determine if the FPGA that responses to the challenges is the FPGA we expect.*

**