Manasa Kiran Ravi Kiran mr4528
Chandrakiran Mettu cm4233

HARDWARE SECURITY

LAB-6

IMPLIMENTATION OF PUF USING RING OSCILLATORS

LAB DUE: 4/25/2017

Manasa Kiran Ravi Kiran mr4528
Chandrakiran Mettu cm4233

Implementation:

We have used implemented Physical unclonable Function using Ring oscillators in accordance with fig 1 below. 4 identical ring oscillators are used for this function.

Ideally as all the RO produce same oscillations all should produce same frequency, irrespective of the selection line all should produce same output as 1's or 0's according to the implementation by the designer.

But due to the process variation, the placement of RO , delay in MUX, path delay and operation of each LuT's differ , thus resulting in different frequencies.

All the RO are connected to two 2:1 MUX, with different user's input different RO are selected. Accordingly, Frequency is calculated by using the separate counters which calculates the frequency of the pair of RO selected.

As the oscillators which are nothing but clock takes minimum time to stabilize, a slow clock is designed to create delay of 10Mhz using system clock of 100Mhz.

After this delay the frequency of the selected RO calculation is performed by the counters and a compotator is used to compare the frequencies of RO's , accordingly the truth table is created which outputs which is faster with reference to the other.

This module is implemented multiple times with accordance with the number of bits needed for the secret key.

Here in our implementation we have 4 such implementations, thus there are 4! Ways results can be generated.

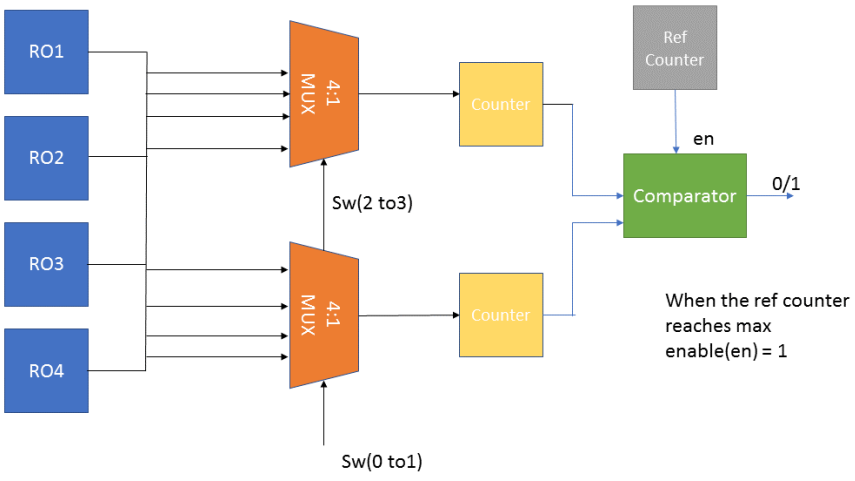

Fig1 : PUF with RO implementation block diagram

Observation:

Ideally running the bit files same key should be generated by all FPGAs. But we see that for each challenge pair different keys are generated by different boards.

The reason for this behavior is, though all belong to same family and operate at same frequency, the process variation differs. By the experiment, we have also found that different LUT's of same board produce different frequency which indirectly says that process variation is different, they all have different delays.

This Vulnerability is exploited in good way to create cryptographic keys in an easy way instead of using complicated algorithms like AES, DES or RSA.

We have updated the challenge pair response on the excel sheet.