**SHORTCOMING OF ANDERSON’S PUF**

INTRODUCTION:

Anderson’s Puf design for Virtex-5(model XC5VLX50-IFFG324) is analysed and found that its not good to use for security critical use. The PUF design from Anderson’s is analysed and its seen that it produces a glitch in the output of the flipflop. The placement of the LUT can influence the Glitch quality.

Analysis and redesign of the Anderson’s PUF:

1-bit PUF output is held by a flip flop initialised to 0. The flip flop content will irrevocably change to 1 wherever a glitch occurs on the asynchronous preset input. The routing path from the output of carry chain multiplexers to thee flip flop preset input can be regarded as a low pass filter. The analysis said that glitches of short duration are not enough to trigger the flip flop.

Having these practical contraints in mind, we cannot expect a stable response from the PUF and instead it will be just a constant output from the PUF. When we increase the number of bits then we can see that we can see a that a lot of switches are switching to ‘1’. This result shows that the responses whose hamming weight increases as time progresses (known as ‘Saturation’).

To overcome the Constant glitch problem, we have two solutions:

1) **Measurement after a specific delay:**

one approach is to eliminate the saturation problem is to latch the PUF output at a single point of time. This is usually done at power on so that the application can use it straight away. The idea to store PUF response at a later point in time so that response is close to being uniformly distributed without the need for key extraction. This approach implies a trade-off between latency and quality.

The results relate to sampling the PUF after .5 sec after power on, then using the response at a variety of times thereafter. The stability of the responses is important, and it gives a good variation of inter and intra distance variation.

2) **A One-shot approach:**

This approach is to store the response immediately after power-on. As mentioned in previous section, there is considerable bias towards 0 at this point for the original PUF design. In the proposed LUT Placement, glitches tend to have a short duration, meaning they are damped out while passing the first time through the routing network as a low pass filter.

Therefore, we control he glitch width transitions between LUT0 and LUT1, increasing it so the probability that a glitch occurs at a preset input of flipflop is also increased. This can be realised by adding an additional carry chain between the two LUT’s. This approach implies a trade-off between area (additional LUT to increase the extended carry chain) and flexibility (range of variation possible).

**FUTURE RECOMMENDATIONS:**

1) We can further investigate that if we need any modification for the original Anderson Design by changing the glitch value from ‘1’ to ‘0’. This will give a more robust design with better properties.

2) Furthermore we can investigate whether the saturation effect itself is an intrinsic property of an FPGA device.