**PRO’s And CONC’s OF PUF:**

1. **MUX PUF**:

PRO’s:

* Delay based PUF [1] which works on giving an N input challenge and getting an N different types of responses for each challenge.

CONC’S:

* It can be attacked by Machine Learning Modelling Attacks.

2. **ANDERSON PUF**:

PRO’s:

* It can be used in FPGA’s and can be secured by manufacturing variations.

CONC’S:

* It can be attacked by Machine Learning Modelling Attacks.
* Saturation problem is there. So that it should be used after 0.5 sec of power on only.
* One- shot Approach to control glitch transition between LUT0 and LUT1. If we add an extra LUT we can eliminate the glitch.

MACHINE LEARNING BASED MODELLING ATTACKS:

ML Algorithm is used to predict the output responses to unknown challenges by training machine learner with a subset of known CRP’s. Take the Arbiter PUF for example with propagation delay path for each switch with two input ports and two output ports be represented as Att,Abt,Ath and Abb where t and b denote the top and bottom ports respectively. Let C[i] = {-1,1} denote the bipolar encoded challenge bit of the ith switch. Assume straight mode as c[i]=1 and swapped mode as c[i]=-1.

Since an ordinary arbiter PUF can be easily predicted by a few hundred CRPS’s by modelling machine learning attacks which we discussed above.

As a counter measure against this attack, non-linear effect can be added, for example by XORing the responses of multiple arbiter PUF’s. It‘s hard to find because we are adding non-linear elements to the Arbiter PUF.

**BUTTERFLY PUF**:

PRO’s:

* Provides bit stream encryption.
* IP Protection on FPGA’s.

CON’s:

* It can be attacked by Machine Learning Modelling Attacks.

EXPERIMENTAL VALIDATION:

Two broadly used validating the output of PUF Response:

* Within Class Variation in Hamming Distance.
* Between Class Variation in Hamming Distance for measurements.

References:

1. Yingjie Lao and Keshab K. Parhi, “Reconfigurable Architectures for silicon Physical Unclonable functions”.
2. Jason H. Anderson,” A PUF Design for Secure FPGA Based Embedded Systems”.
3. Chip Hong Chang, Yue Zheng and Le Zhang, “A Retrospective and a Look Forward: Fifteen Years of Physical Unclonable Function Advancement”.