Design and Analysis of Mux-based Physical Unclonable Functions

Rahim Pegu[1]
Department of Electronics and Communication
School Of Technology,NEHU
Shillong, Meghalaya.

Rajkishur Mudoi[2]
Department Of Electronics and Communication
School of Technology,NEHU
Shillong, Meghalaya.

***Abstract*— Physical Unclonable Functions (PUFs) is an interestingly new circuit development in the field of hardware security. It takes the advantage of the uncontrollable intrinsic random features of physical objects during manufacturing process. The PUFs provides significantly higher identification and authentication by incurring hidden information from perplexed properties of physical material instead of storing them in non-volatile memory. The previous works perform the rigorous statistical analysis of the different types of MUX-based PUFs in PSPICE environment in 65nm technology process. This paper presents the well experimented analysis of the different MUX-based PUFs which is based on layout-based simulation performed in CMOS 50nm.rul. These experiments are carried out in Microwind and DSCH 2.7 tool. The MUX-based PUFs includes Basic MUX, Standard feed-forward MUX, Modified feed-forward Overlap MUX and MUX-DeMUX PUF. The performance metrics of different PUFs are expressed in terms of Intra-chip variation, Inter-chip variation, Reliability, Uniqueness, Randomness. It is clear from the experiment that Basic MUX PUF gives the best reliability among all of the PUFs, but as the number of stage increases the reliability decreases. Uniqueness and randomness increase as the number of stages increase in Basic MUX PUF. In the both standard feed forward and Modified feed forward overlap PUF, reliability decreases compared to basic MUX PUF, but both uniqueness and randomness increases. If we observe, it is seen that modified feed forward overlap PUF provides more reliability than standard feed forward, but having lesser uniqueness and randomness. In this paper, we introduce a novel PUF, named as "Feed-forward-MUX/DeMUX" which is analyzed in 0.6μm technology process, in DSCH 2.7. Here, we analyze only the static challenge-response behavior of the PUF. The analysis presented in this paper will allow the designer to choose PUF based on application requirements without going into fabrication steps.**

Keywords—Physical Unclonable Function(PUF); Intra-chip Variation; Inter-chip Variation; Reliability; Uniqueness; Randomness; Standard feed forward; Modified feed forward overlap.

I. INTRODUCTION

I.I.PHYSICAL UNCLONABLE FUNCTION

Now-a-days, smartphone and embedded devices are becoming omnipresent and interconnected platform for everyday tasks such as banking, healthcare, supply chain and transportation etc. During such tasks, it is very crucial that the mobile devices have to securely authenticate or be authenticated by another troupe and securely deal private information. On the other hand, the counterfeiting problem has been increasing day by day from different perspectives such as integrated circuit design, different branded products etc. This problem leads not only losses to any industry or brand image, but also threats to national defense and human being. Therefore, the PUF have been introduced which is defined as the randomized physical system that can be challenged with so called external stimuli, upon which it reacts with corresponding response. These responses depend on the micro or nanoscale structural disorder of PUF manufacturing process variation and somewhat on environmental variation.

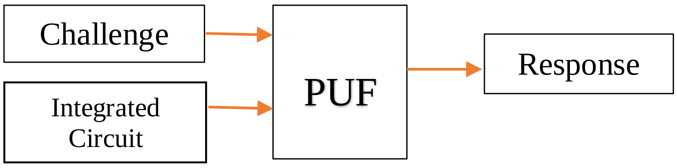

Fig: 1 Block diagram of Physical Unclonable Function

It is assumed that the disorder cannot be cloned or reproduced exactly, not even by the original manufacturer of the PUF with exact known feature. This means that each and every PUF has a unique identification like fingerprint of human being. The PUF is embedded in physical device in an inseparable way as shown fig.1, for secure identification of the device to be identified. Due to uncontrollable random component, PUFs are easy to measure but hardly clone, predict or reproduce practically. Moreover, it is impossible to mount an invasive attack to copy secret information without changing physical randomness. Because of these advantages, PUFs can be applied in cryptographic application for generation of efficient and reliable secret key; and enables low cost authentication of ICs (Integrated Circuits).

This paper presents the performance of various kind of PUFs in terms of three performance factors i.e. Reliability, Uniqueness, Randomness. The performances of PUFs are manufacturing process and environment dependent. The reliability of PUF captures how efficiently a PUF is producing the same output response of an IC chip. The responses of multiplexer-based (MUX-based) PUFs are expected to be identical with respect to the same challenge applied repetitively. The ability of a PUF to uniquely recognize a particular chip among a group of chips of the same type is signified by uniqueness. Different output responses are expected for different PUFs with respect to same applied challenges. Ideally, the Hamming distance between the responses of different PUFs should be 50% [1]. Randomness represents the unbiasedness of the PUF response.

It would be helpful for designers to predict the performance comparisons among different PUF designs by acquiring the knowledge of the process variation pattern and variation of circuit parameters (e.g., threshold voltage, delay etc.) before fabrication process. In this paper, we applied typical, minimum, maximum and Monte-Carlo process variation during simulation of various types of PUF designs.

I.II. LITERATURE SURVEY AND OUR CONTRIBUTION

The Optical PUF [2] is the first PUF, where the randomness in the position of the light scattering particles and the complexity of the interaction between the laser and the particles are applied. In [3], entropy analysis of optical PUF has been discussed. After Optical PUF, several PUF hardware structures have been proposed [4–8]. The statistical models of ring oscillator PUF [9], [10] and MUX PUFs [11]–[13] have also been studied in the literature. Additionally, a relation between the statistical analysis of PUFs to circuit-level optimization and architecture-level optimization is presented in [14], which leads to interesting results that could improve the design and implementation of reliable and efficient PUFs.

The objective of this paper is to compare the various types of silicon PUFs based on experimental data analysis and to predict the relative advantages among the PUFs. In previous works [1], presents the theoretical and experimental comparison of the performance of different MUX-based PUFs. In some respects, the work in this paper can be differentiated from existing efforts. To the best of our knowledge, this paper presents the systematic experimental analysis which is layout based, performed using Microwind tool. The PUFs include basic or Original PUF [1], Standard Feed Forward PUF and Modified Feed Forward Overlap PUF [1]. In addition, we also introduce a novel PUF by combining the both Standard Feed Forward [1] and MUX/DeMUX [1] PUF structure, namely, Feed-Forward-MUX/DeMUX. Moreover, in this paper, we applied two clocks having different frequency from two inputs instead of using rising edge input [1]. We also analyzed this PUF and MUX/DeMUX experimentally by DSCH 2.7 tool in 0.6μm technology.

I.III. PAPER ORGANIZATION

The remaining part of this paper as follows. In section II we introduce background of Silicon PUF, Feed Forward, Modified Feed Forward and MUX/DeMUX Structure. In Section III, we present the novel Feed-forward-MUX/DeMUX PUF structures. Section IV, includes the definition of performance metrics i.e., Reliability, Uniqueness, Randomness. Section V describes the methodology for modelling of PUF and simulation model. Section VI shows the performance comparison of Original MUX, Standard feed forward, and Modified feed forward overlap PUF structure. In Section VII, we finally conclude the paper with the performance analysis of the MUX/DeMUX, Feed Forward-MUX/DeMUX Structure.

II BACKGROUND

II.I. SILICON PHYSICAL UNCLONABLE FUNCTION

Silicon Physical Unclonable Functions came in existence with the notion of Physical Random Functions (PRFs). A Physical Random Function [4] is defined to have the following properties.

1. A physical random function is a function that maps challenges to responses, the challenge response pairs being characteristic of the physical device (e.g., IC).
2. The evaluation of challenge response pairs can be easily done in a short period of time.
3. But it is not easy to characterize with the knowledge of a set of challenge response pairs. An attacker with a polynomial amount of resources could not be able to model the challenge response behavior of the PRF.
4. The PRF is manufacturer resistant or "physically unclonable" as it is impossible to produce two identical devices with the same physical properties.

The design of Silicon PUF circuits can be guided by above four properties. There are two main types of delay-based silicon PUFs: Ring Oscillator (RO) PUF [15] and Multiplexer (MUX) PUF [16]. However, the MUX PUF is more secure than the RO PUF, as attackers can evaluate easily the frequencies of the ring oscillators; moreover, a MUX PUF is more suitable for resource-constrained applications. We can use N different challenges to obtain an N-bit long response in a MUX PUF, shown in figure 2, rather than duplicating the hardware N times as in an RO PUF. This kind of silicon PUF consists of N stages MUXs and one arbiter, as shown in figure 3, which connects the final stage of the two paths. MUXs in each stage acts as a switch to either straight or cross propagate the two input signals of different frequencies, with respect to the corresponding challenge bit. Usually, designing of each MUX is done equivalently, but the manufacturing process leads to variations in it. Finally, the arbiter translates the analog timing difference into a response (either 0 or 1). For transistors, manufacturing variability exists due to variations in transistor length, width, gate oxide thickness, doping concentration density, metal width, metal thickness, and ILD (inter-level dielectric) thickness etc. [18].

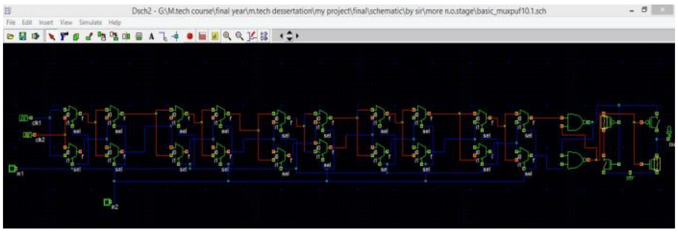
Dsch2 - G:\M.tech course\final year\m.tech dessertation\my project\final\schematic\by sir\more n.o.stage\basic_muxpuf10.1.sch

Fig. 2: A 10-stage Original MUX PUF (Silicon PUF) design in DSCH

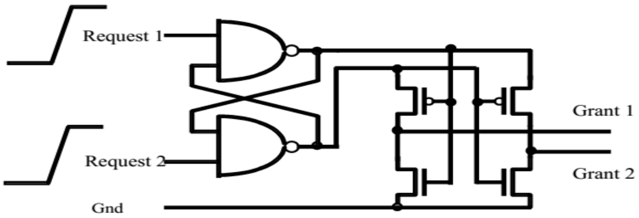

Fig.3: Arbiter circuit [17]

II.II. FEED FORWARD STRUCTURE

A feed forward structure of silicon PUF proposed in [19] to preclude the linear modelling attacks. Figure 4, shows one basic structure of feed-forward MUX PUF, where result of an intermediate stage acts as the select signal for a block of MUXs in a later stage. This structure increases the non-linearity to the original MUX PUF, simultaneously increases the complexity for numerical modeling attacks [20]. However, the reliability of the PUF has been degraded. The reason is that an error in the output of an internal feed-forward arbiter caused by environmental variation can increase the noise probability in the final response [1].

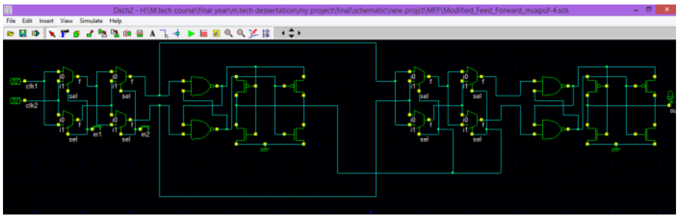
Dsch2 - H:\M.tech course\final year\m.tech dessertation\my project\final\schematic\new projct\MFF\Modified_Feed_Forward_muxpuf-4.sch
File
Edit
Insert
View
Simulate
Help
clk1
clk2
sel
in1
in2

Fig.4: Standard 4-stage feed forward structure

II.III. MODIFIED FEED FORWARD STRUCTURE

In [1], modified feed-forward MUX PUF structure was introduced and three types of structure have been proposed, i.e., Modified Feed Forward Cascade, Modified Feed Forward Overlap, Modified Feed Forward Separate. An instance of Modified feed forward overlap (MFFO) is shown Figure 5.

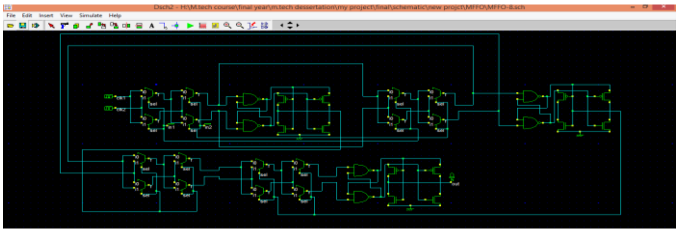
Dsch2 - H:\M.tech course\final year\m.tech dessertation\my project\final\schematic\new projct\MFFO\MFFO-8.sch
File
Edit
Insert
View
Simulate
Help

Fig.5: An instance of 8-stage modified feed forward overlap structure

In the modified feed forward structure [1], the output of a feed-forward arbiter from an intermediate stage is input as a challenge bit for a block of MUXs in a later stage. By employing the modified feed-forward path, the reliability of the feed forward structure can be improved [1]. In this paper, only Modified Feed Forward Overlap structure is analyzed because, according to the paper [1], this structure provides more improved results comparatively to the standard feed forward and other modified feed forward structures.

II.IV. MUX/DeMUX STRUCTURE

This structure first introduced in [21]. Here, DeMUX is used to select the direction of the propagating signal, and makes the PUF reconfigurable. We can skip some stages by adding DeMUX components, instead of propagating the signal of different frequency successively, which could make the challenge response behavior reconfigurable and hard to predict.

The basic reconfigurable MUX/DeMUX structure is shown in figure 6.

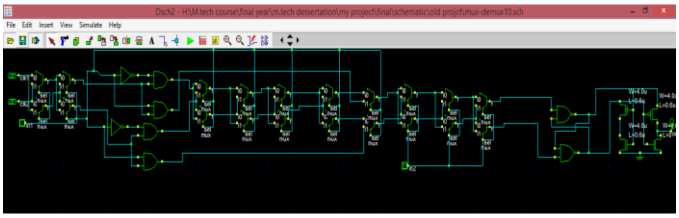
Dsch2 - H:\M.tech course\final year\m.tech dessertation\my project\final\schematic\old projct\mux-demux10.sch
File
Edit
Insert
View
Simulate
Help
clk1
clk2
in1
sel
mux
W=4.0u
L=0.6u

Fig.6: An instance of *MUX/DeMUX STRUCTURE of 10-stage*

III. FEED-FORWARD-MUX/DEMUX PUF

Based on the Feed Forward and MUX/DeMUX variability [1] and reconfigurable property [21]; in this paper, we propose a novel 'feed-forward-MUX/DeMUX' structure shown in Fig. 7. This logic reconfigurable PUF structure is designed by combining both standard feed forward and MUX/DeMUX PUF structure. This structure utilizes both the features of standard feed forward and MUX/DeMUX PUF together, where the result of an intermediate stage acts as the select signal for a block of MUXs in a later stage and MUX/DeMUX structure can choose to skip some stages or vice versa. This structure provides more non-linearity to the original PUF structure compared to the standard feed forward or MUX/DeMUX structure. This non-linearity makes the circuit more secure from numerical modeling attack.

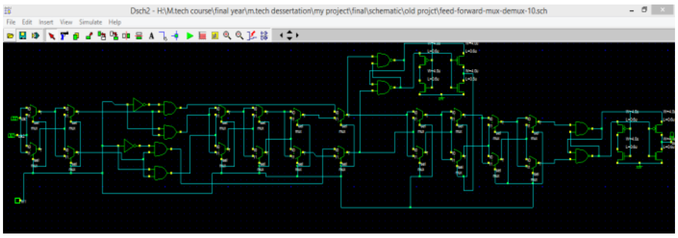
Dsch2 - H:\M.tech course\final year\m.tech dessertation\my project\final\schematic\old projct\feed-forward-mux-demux-10.sch
File
Edit
Insert
View
Simulate
Help
sel
mux
W=4.0u
L=0.6u

Fig.7: An instance of 10-stage Feed-forward-MUX/DeMUX PUF

IV DEFINITION OF PUF PERFORMANCE METRICS

In this section, as in [1], we define three PUF performance metrics to obtain the performance of various MUX-based PUFs. The main concern of this paper is the relative performance analysis rather than the absolute value of each indicator.

A. Reliability

The intra-chip variations is measure of reliability of PUFs which is determined by comparing the analog signatures of the PUF with respect to same challenge under different environmental conditions [1]; in our case, we consider the temperature as the primary environmental factor. Let P_{intra} represent the probability that a certain time of 1's response will flip when applying a randomly selected challenge multiple times. Therefore, P_{intra} can be used to represent the intra-chip variation for the entire L-sec response. In particular, the average Hamming Distance (HD) between the responses is used for variations of MUX-based PUFs. The P_{intra} and average HD defined by [1]

$$E\ (HD_{intra}) = P_{intra} = E(\frac{1}{m}\sum_{i=1}^{m}\frac{HD(R,R')}{L} \times 100\% ....(1)$$

Where m is the number of HD comparisons, and R and R' represent two measurements of the PUF response under different conditions. Therefore, Reliability can be defined as follows [1].

$$Reliability = 1 - P_{intra} \quad ……………………………… (2)$$

B. Uniqueness:

The inter-chip variation [1] is a measure of uniqueness which is evaluated by comparing the hamming distance between two analog signatures which are generated by a same challenge and configure data from different chips. We can define *Pinter* as the probability that the output generated by the same challenge for different PUF instances are different. Since uniqueness is a measure of inter-chip performance, all possible chip combinations should be considered. Therefore, the average inter-chip HD of *K* PUFs can be described as [1]

$$E\ (P_{inter}) = P_{inter} = E\ (\frac{2}{K(K-1)}\sum_{i=1}^{K-1}\sum_{j=i+1}^{K}\frac{E(R(i),R(j))}{L} \times 100\%) \quad …………… (3)$$

Since *Pinter* = 50% represents the best uniqueness for a PUF, the uniqueness indicator can be defined by [1]

$$Uniqueness = 1 - |2 \times P_{inter} - 1| \quad ………………………(4)$$

C. Randomness

A MUX PUF is expected ideally to produce unbiased 0's and 1's. Randomness represents the ability of the PUF to output 0 and 1 response with equal probability. One measurement of the randomness can be expressed as [1]

$$Randomness = 1 - |2 \times P(R = 1) - 1| ………………… (5)$$

The value of $P(R = 1)$ which is more close to 0.5 indicates better randomness.

V. METHODOLOGY

V.I. PHYSICAL UNCLONABLE FUNCTION MODELLING

A MUX PUF can consist of N-stages MUX and one arbiter, as shown in figure 2 (shown 10-stages). The two clock signals of different frequency stimulate two input simultaneously. The challenges or select lines determine the actual path of propagation of the two signals. After the last stage, the arbiter compares the analog timing difference between the two signals and produce output signature (IDs). It becomes standard to model the MUX PUF via an additive linear delay model [12]. Statistical Static Timing Analysis [18], tells that the manufacturing process parameter variations for transistors can be modeled by a Gaussian distribution. Therefore, the variations of delay will also be approximately Gaussian [21]. Manufacturing process variations can be classified in two categories [21]:

1. Inter-die variations
2. Intra-die variations.

Inter-die variations signifies the parameter variations that affect all devices equivalently across a single die, while intra-die variations means the parameter variation that have different effects on the devices within the same chip. To increase the accuracy of the concern model, we need to consider the correlation of these variation. In the Grid model [18], assume that there is high correlation among the devices in nearby grids and low correlations in faraway grids, as manufacturing process variations are more likely to have similar effects on closer devices. It is also shown that the inter-chip variation across the wafer is similar to that within a single wafer [16]. In addition, the output of the arbiter in silicon PUF is only based on the delay difference of two selected paths [21]. Therefore, the inter-chip variations mainly contribute to the randomness of response for each IC, while die-to-die and wafer-to-wafer manufacturing variations will have minimum effect on the output response.

We usually design every multiplexer equivalently in a MUX PUF; therefore, the delay of each single MUX can be modelled as independent identically distributed random variable D_i. This follows normal distribution, N (μ, σ^2); therefore, the total delay of the N stages will be N $(N\mu, N\sigma^2)$. Since the output of arbiter will only depend on the delay difference (Δ) between the two paths, the time difference will also follow a Gaussian distribution [21]

$$\Delta \sim N\ (0;\ 2N\sigma^2).$$

If we denote the delay in the top path of *i-th* stage as D_{t_i} the delay in the bottom path of *i-th* stage as D_{b_i}, and the challenge bit for each stage as C_i. Thus, the delay difference of *i-th* stage will be [21]:

$$D_{t_i}\text{-}D_{b_i} \sim N\ (0;\ 2N\sigma^2)$$

Then if the challenge is 0, then the delay difference added into the whole paths will be D_{t_i}-D_{b_i}; otherwise, if the challenge bit for *i-th* stage is 1, the additive delay difference will be D_{b_i}- D_{t_i}

It can be expressed as [21]:

$$\Delta_i = \ (-1)^{C_i}(D_{t_i}\text{-}D_{b_i}) \sim N\ (0;\ 2N\sigma^2)$$

As a result, the arrival time difference between the two inputs of the arbiter is [21]:

$$\Delta_t = \sum_{i}^{N}(-1)^{C_i}(D_{t_i} - D_{b_i}) \sim N\ (0;\ 2N\sigma^2)$$

Thus, the final response is [21]:

$$R = \text{sign}\ (\Delta_t)$$

Where we use the convention that

$$R = \text{sign}\ (\Delta_t) = 0;\ \text{where}\ \Delta_t < 0;$$
$$R = \text{sign}\ (\Delta_t) = 1;\ \text{where}\ \Delta_t \geq 0;$$

V.II SIMULATION MODEL

In this paper, we applied simulation method to test and analyze the different performance metrics rather than fabrication method. In our simulation, for manufacturing process variations, we apply the Gaussian model which has been explained in Section V.I. The Microwind 2.7 works on lambda grid not in micro grid. For simulation, we set up the process parameters variation manually in the Microwind. We applied empirical level of MOS model, and typical, minimum, maximum, Monte-Carlo (normal distribution) for process variation in Microwind. Our simulation result of inter-chip variation leads to a Hamming distance range from average value of 12% to 53.7% for original PUF, while the intra-chip variation is from 0.168 % to 10.127% on average. The results are not absolute but relative performance would be useful. These results are also acceptable, if we observe previous published results. Thus, we believe that our simulation delay model is consistent with the industrial manufacturing process variations.

VI. PERFORMANCE MEASUREMENT OF BASIC MUX AND STANDARD FEED FORWARD AND MODIFIED FEED FORWARD OVERLAP MUX PUF

1) *Performance Analysis of Basic MUX PUF*

Here, we have taken 30-stage basic MUX PUF showing the way of measurement of the different performance metrics. The following figure 8.a and figure 8.b shows the schematic and layout of 30-stage basic MUX PUF respectively in which analog simulation is performed in CMOS 50nm.rul in Microwind. Two clock signals with different frequency will excite the two parallel paths simultaneously. The actual propagated paths will be determined by the external applied challenge bits which are forced through 4-select line i.e., in1, in2, in3, in4.

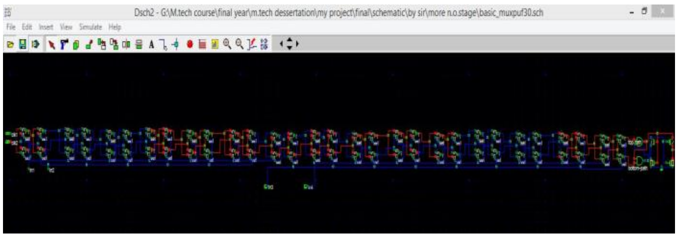
Dsch2 - G:\M.tech course\final year\m.tech dessertation\my project\final\schematic\by sir\more n.o.stage\basic_muxpuf30.sch
File Edit Insert View Simulate Help

Fig.8.a: Schematic of 30-stage original MUX PUF

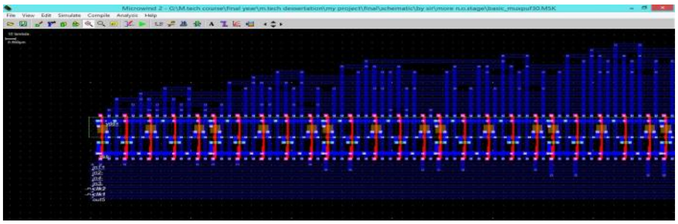
Microwind 2 - G:\M.tech course\final year\m.tech dessertation\my project\final\schematic\by sir\more n.o.stage\basic_muxpuf30.MSK
File View Edit Simulate Compile Analysis Help

Fig.8.b: A section of layout of the 30-stage Original MUX PUF

In the experiment, Monte-Carlo ($\pm$20% normal distribution) process variation is exploited which consist of altering two main parameters: the threshold voltage (20% random variation, Gaussian distribution) and the mobility (20% random variation). All other parameters are supposed to be constant. The MOS Model 3(empirical level) of Microwind tool is used, where typical carrier mobility $\mu_{o,nmos}$=0.06 m^2/V.s and $\mu_{o,pmos}$= 0.025 m^2/V.s and threshold voltage $V_{to,nmos}$= 0.4V $V_{to,pmos}$= -0.4V. It has been seen in our experiment that the intra-chip variations introduced by different temperatures were more significant. The analog signature of the PUFs at 10^{0}c, 30^{0}c, 50^{0}c, 70^{0}c and 100^{0}c are obtained and shown in figure 9.a, 9.b and 9.c. The comparisons were done with each other for each select line combination. However, we only present the comparisons between the two temperatures, which exhibit the largest variations. Here, for final intra-chip variation, average value of intra-chip variation for all select lines combination were taken. In two 30-stage PUF instance, 16 combination of select input applied, where total of 120*2=240 comparisons are performed. For inter chip variation, in each PUF instance we applied the three process variations, namely, minimum, typical and maximum for each challenge input, i.e. K=3; which gives three comparison with each other. Therefore, in 30-stage PUF, we made total of 3*16*2=96 comparisons. The 2 indicates the number of PUF instance taken. Then, we took the average inter-chip variation for the PUF instance. After calculation of the intra-chip and inter-chip variation, we can find out the Reliability and Uniqueness. Randomness is found by averaging the probability of getting response ‘1’ for all challenges. Similarly, we performed the analysis of 20 and 50-stage original mux PUF.

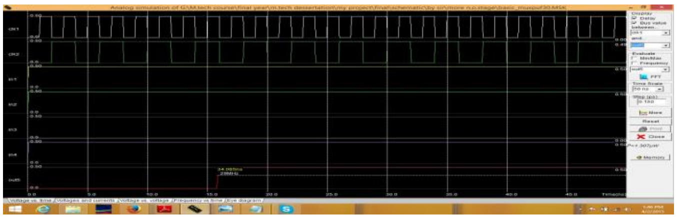

Fig.9.a: Analog simulation output performed at 10 ^{0}c at in1=1, in2=1, in3=0, in4=1

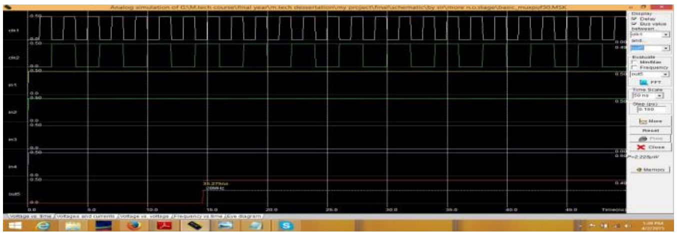

Fig.9.b Analog simulation output performed at 30 ^{0}c at in1=1, in2=1, in3=0, in4=1

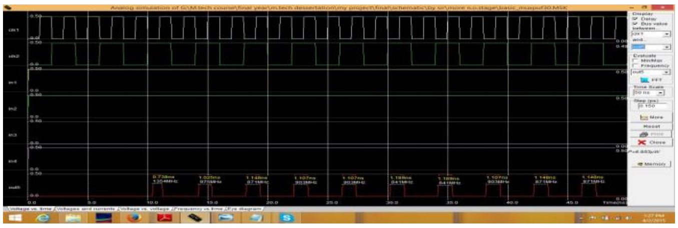

Fig.9.c Analog simulation output performed at 50 ^{0}c at (in1=1, in2=1, in3=0, in4=1)

Discussion:

It has been seen from the table I that reliability decreases as the no. of stage increases that can be compared with previous theoretical and statistical analysis result [1]. It is also seen that

Uniqueness and Randomness are increasing, which makes it more secure PUF. Again, it is seen that inter-chip variation is larger than intra-chip variation, thus we can observe that the variations caused by the randomness in manufacturing process are more significant than the variations under different environmental conditions. The results obtained are not absolute, but can be used for performance comparison.

TABLE I
Performance metric table after experimental analysis for different stage of Original MUX PUF in Microwind and DSCH 2.7

No Of Stage	Intra-chip Variation avg. (%)	Reliability avg. (%)	Inter-chip avg. Variation (%)	Uniqueness avg. (%)	P(R=1) avg. (%)	Randomness avg. (%)
20	1.91	98.01	33.72	67.44	15.13	30.26
30	4.43	95.56	35.76	71.53	22.16	44.32
50	10.00	90.00	42.80	85.60	39.36	78.72

TABLE II
Performance metric table after experimental analysis of Standard feed forward and Modified feed forward MUX in Microwind and DSCH 2.7

Name of PUF	No Of Stage	Intra-chip Variation (%)	Reliability (%)	Inter-chip Variation %)	Uniqueness (%)	P(R=1) (%)	Randomness (%)
Standard Feed-forward MUF	30	11.527	88.473	39.928	79.857	43.050	86.10
Modified feed forward MUX	30	9.754	90.250	33.002	66.040	34.200	68.40

2. *Performance Analysis of Standard feed forward and Modified feed forward overlap MUX PUF*

Here, we performed experiment of 30-stage PUF circuit for the feed forward MUX PUF analysis as shown in fig.10.a and 10.b.

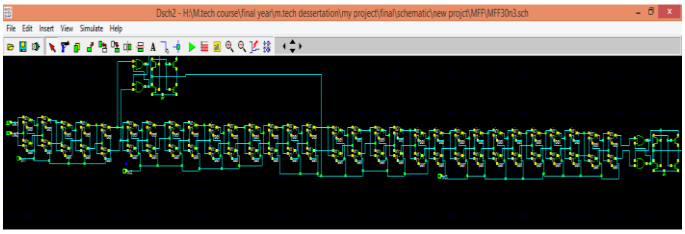
Dsch2 - H:\M.tech course\final year\m.tech dessertation\my project\final\schematic\new projct\MFF\MFF30n3.sch
File Edit Insert View Simulate Help

Fig.10a: Schematic of 30-stage Standard Feed Forward MUX

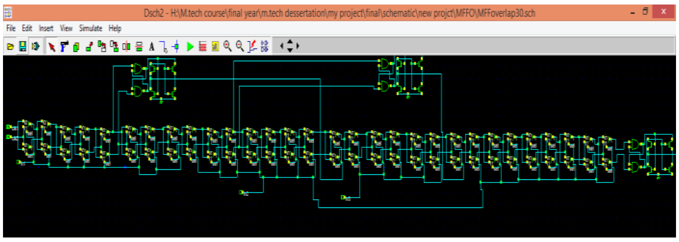
Dsch2 - H:\M.tech course\final year\m.tech dessertation\my project\final\schematic\new projct\MFFO\MFFoverlap30.sch
File Edit Insert View Simulate Help

Fig.10b: Schematic of 30-stage Modified Feed Forward Overlap MUX PUF

Similarly to the Original MUX PUF, we performed the experiment in CMOS 50nm.rul. Here, for intra-chip and inter-chip variation, we performed experiment of 5 different PUF instance for each MUX PUF. For intra-chip variation, we did 5*28=140 comparison considering 3-select input for each PUF instance. For inter-chip variation, we performed similar to the Original MUX PUF, but 5 different PUF instance are considered. Therefore, total 3*5*8= 120 comparisons are done.

Discussion:
From the above table II, it is clear that intra-chip variation lesser in Modified Feed Forward Overlap (MFFO) Structure in comparison with Standard Feed Forward (SFF) PUF. This reveals that reliability is increased by MFFO, but less secure. The results obtained are not absolute but relative performance analysis can be performed.

VII.I PERFORMANCE MEASUREMENT OF MUX/DEMUX AND FEED FORWARD-MUX/DEMUX PUF

We performed these experiments only for analysis of static challenge-response behavior, which is performed in 0.6um technology of DSCH 2 tool. Here, there are no environmental variation and process variation. In the experiment, for both MUX/DeMUX and FFMD PUF, the intra-chip variation is measured by comparing the response among the different challenges. The schematic of 30-stage MUX/DeMUX, FFMD and 100-stage FFMD are shown in fig. 11, 12a, 12b respectively. The fig.13a and 13b shows the timing diagram of output with respect to challenges. In the 30-stage MUX/DeMUX and FFMD for Intra-chip variation, we did 5*28=140 and 5*12 comparison respectively; but, in case of 100-stage FFMD PUF, we did 2*120 comparison considering two FFMD PUF instance. Two timing diagram of 100-FFMD PUF is shown in fig.14a. and 14b. For inter-chip variation, in the 30-stage MUX/DeMUX and FFMD, we performed 8*10 and 4*10 comparison respectively; but in 100-stage FFMD PUF 16 comparisons were done. We have calculated the probability of getting response 1, P(R=1) by taking the average of the output response of getting '1' with respect to all possible challenges. Hence, randomness is calculated by equation (5).

Discussion: From the table III, it can be inferred that the intra-chip variation of 30- stage FFMD is lesser than MUX/DeMUX, but if we increase number of stage it decreases as shown in the 100-stage FFMD. But Inter-chip variation and Randomness increases as the number of stage increases which made this FFMD circuit more secure.

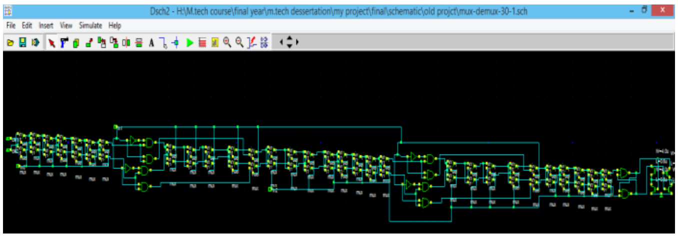
Dsch2 - H:\M.tech course\final year\m.tech dessertation\my project\final\schematic\old projct\mux-demux-30-1.sch
File Edit Insert View Simulate Help

Fig.11: Schematic of 30-stage MUX-DeMUX PUF

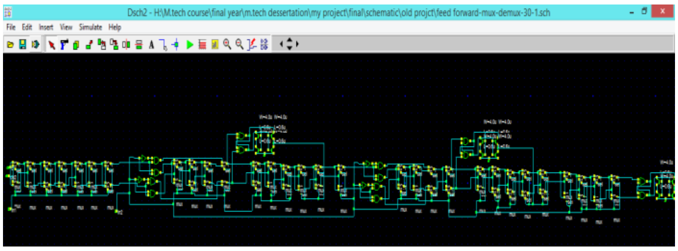
Dsch2 - H:\M.tech course\final year\m.tech dessertation\my project\final\schematic\old projct\feed forward-mux-demux-30-1.sch
File Edit Insert View Simulate Help

Fig.12a: Schematic of 30-stage of FFMD

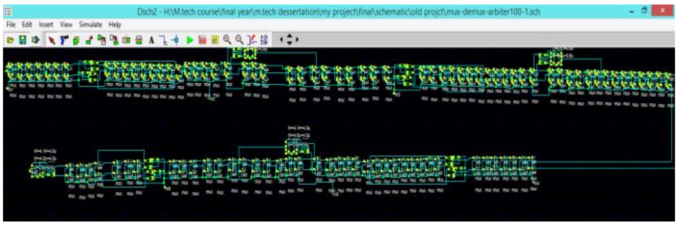
Dsch2 - H:\M.tech course\final year\m.tech dessertation\my project\final\schematic\old projct\mux-demux-arbiter100-1.sch
File Edit Insert View Simulate Help

Fig.12b: Schematic of 100-stage of FFMD

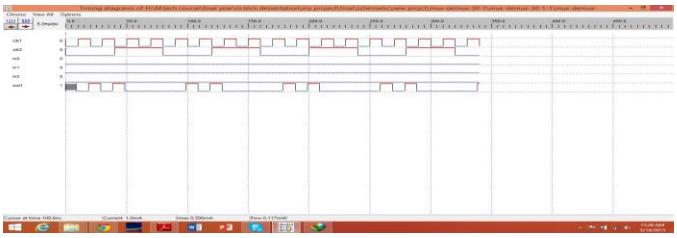

Fig.13.b: Timing diagram of 30-stage MUX/DeMUX with challenge in0=0, in1=0, in2=0

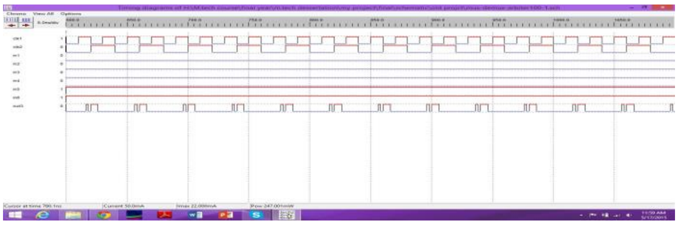

Fig.14a: Timing diagram of 100-stage FFMD with challenge in1=0,in2=0,in3=0,in4=0,in5=in6=1

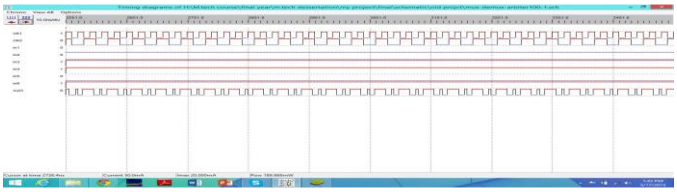

Fig.14b: Timing diagram of 100-stage FFMD with challenge in1=0,in2=0,in3=1,in4=1,in5=0,in6=1

VI. II. CONCLUSION

We have presented the comparative study of various MUX-based Physically Unclonable Function by executing optimum number of experiments. The experimental results effectively reflects the characteristics of various PUF designs in terms of three performance metrics i.e. Reliability, Uniqueness, Randomness as shown in table I and II. We also proposed a novel structure ‘Feed Forward-MUX/DeMUX’ which is analyzed by observing static challenge-response behavior. The analysis of ‘Feed Forward-MUX/DeMUX’ based on variation of process and environmental variation and statistical analysis will be the future work. In addition, future work will be directed towards the evaluation of MUX-based PUFs from a security perspective by various types of modeling attacks.

TABLE III
Performance metric table after experimental analysis for MUX/DeMUX and Feed Forward-MUX/DeMUX in DSCH 2.7

Name of the PUF	No. of Stage	Intra-chip variation (Avg.%)	Inter-chip Variation (Avg.%)	P(R=1) (%)	Randomness (%)
MUX-DeMUX	30	15.990	20.520	37.924	75.848
FFMD	30	14.990	10.000	31.430	62.860
FFMD	100	21.119	15.087	32.027	64.055

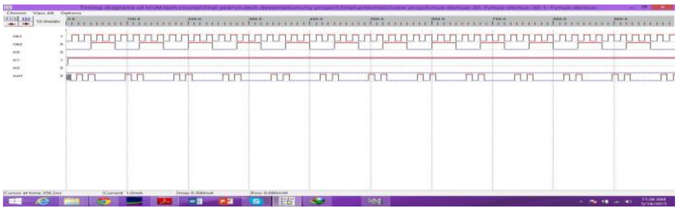

Fig.13.a: Timing diagram of 30-stage MUX/DeMUX with challenge in0=0,in1=1,in2=0

References

[1] Y. Lao and K. K. Parhi, “Statistical analysis of Mux-based Physically Unclonable functions,” *IEEE Transactions. Computer-Aided Design integtaed circuit and systems*, Vol. 33, No. 5, May 2014.

[2] R. Pappu, B. Recht, J. Taylor, and Gershenfeld, “Physical One-way functions.” *Science*, vol. 297(5589), p. 2026, 2002.

[3] B. Skoric, “On the entropy of keys derived from laser speckle; statistical properties of Gabor-transformed speckle,” *J. Opt. A: Pure Appl.Opt.*, vol.10, no. 5, p. 055304, 2008.

[4] B. Gassend, D. Clarke, M. V. Dijk, and S. Devadas, “Silicon physical random functions,” *the 9th ACM Conference on Computer and Communications Security*, p. 160, 2002.

[5] B. Gassend, D. Clarke, M. V. Dijk, and S. Devadas, “Controlled physical unclonable functions,” *in Computer Security Application Conference*, 2002,pp. 149-160

[6] S. Kumar, J. Guajardo, R. Maesyz, G. Schrijen, and P. Tuyls, “Extended abstract: The butterfly PUF protecting IP on every FPGA,” *Hardware-Oriented Security and Trust (HOST 2008)*, pp. 67–70, 2008.

[7] R. Maes, P. Tuyls, and I. Verbauwhede, “Intrinsic PUFs from flip-flops onreconfigurable devices,” *in Benelux Workshop Information and System Security (WISSec 08)*, 2008.

[8] D. E. Holcomb, W. P. Burleson, and K. Fue, “Initial SRAM state as a fingerprint and source of true random numbers,” *in Conference on RFID Security*, 2007.

[9] A. Maiti, J. Casarona, L. McHale, and P. Schaumont, “A large scale characterization of RO-PUF,” in *Proc. IEEE Int. Symp. HOST*, 2010, pp. 94–99.

[10] R. Maes, P. Tuyls, and I. Verbauwhede, “Statistical analysis of silicon PUF responses for device identification,” in *Proc. SECSI Workshop*, 2008.

[11] Z. C. Jouini, J. Danger, and L. Bossuet, “Performance evaluation of physically unclonable function by delay statistics,” in *Proc. IEEE 9th Int. NEWCAS*, Jun. 2011, pp. 482–485.

[12] Z. Tariguliyev and B. Ors, “Reliability and security of arbiter-based physical unclonable function circuits,” *Int. J. Commun. Syst.*, 2012.

[13] Y. Hori, T. Yoshida, T. Katashita, and A. Satoh, “Quantitative and statistical performance evaluation of arbiter physical unclonable functions on FPGAs,” in *Proc. Int. Conf. ReConFig*, 2010, pp. 298–303.

[14] I. Kim, A. Maiti, L. Nazhandali, P. Schaumont, V. Vivekraja, and H. Zhang, “From statistics to circuits: Foundations for future physical unclonable functions,” in *Towards Hardware-Intrinsic Security*. Berlin, Germany: Springer, 2010, pp. 55–78.

[15] G. E. Suh and S. Devadas, “Physical unclonable functions for device authentication and secret key generation”, *in ACM/IEEE Design Automation Conference*, pages 9-14, 2007

[16] D. Lim, J. W. Lee, B. Gassend, G. E. Suh, M. V. Dijk, and S. Devadas, “Extracting secret keys from integrated circuits,” *IEEE Transaction on Very Large Scale Integration Systems*, vol. 13, no. 10, p. 1200, 2005.

[17] Synchronizers and Arbiters, Tutorial 7, april, 2008, David kinniment, School of electrical, electronics and computer engineering , University of Newcastle

[18] H. Chang and S. Sapatnekar, “Statistical timing analysis considering spatial correlation in a pert-like traversal,” in *Proc. IEEE Int. Conf. Comput.-Aided Design Integr. Circuits Syst.*, 2003, pp. 621–625.

[19] J.-W. Lee, D. Lim, B. Gassend, G. E. Suh, M. van Dijk, and S. Devadas, “A technique to build a secret key in integrated circuits with identification andauthentication applications,” *in IEEE International Conference Computer-Aided Design Integrated Circuits and Systems*, 2003, pp. 621–625.

[20] U. Ruhrmair, F. Sehnke, J. Solter, G. Dror, S. Devadas, and J. Schmidhuber, “Modeling attacks on physical unclonable functions,” in *Proc.Conf. RFID Security*, 2010, pp. 237–249.

[21] Y. Lao and K. K. Parhi, “Reconfigurable architectures for silicon physical unclonable functions,” *in Proc. IEEE Int. Conf. Electro Inf. Technol.*, 2011, pp. 1–7.

.