# Design of a Low Power Physically Un-clonable Function for Generation of Random Sequence for Hardware Security

Jyotirmoy Pathak    Konsam Jemson Meitei
Department of Electronics and Communication, Lovely Professional University
Phagwara, Punjab (India)

**Abstract**
Physical Un-clonable Function (PUF) is a physical entity that provides secret key or fingerprints in silicon circuits by exploiting the uncontrollable randomness during its manufacturing randomness. It provides a hardware unique signature or identification. Its property of uniqueness comes from its unpredictable way of mapping challenges to responses, even if it was manufactured with the same process. Previous work has mainly focused on novel structures for non-FPGA reconfigurable silicon PUFs which does not need any special fabrication method and which can overcome the limitations of FPGA-based simulations. Their performance was quantified by the inter-chip variations, intra-chip variations and re-configurability tests to meet practical application needs. This paper presents a novel approach of designing a low power non-FPGA feed-forward PUF using double gate MOSFET and also to analyze its parameters such as intra-chip variation, reliability and power.

**Keywords:** Physical Un-clonable Function (PUF); Intra-chip Variation; Reliability; Uniqueness; Standard feed forward; Double gate MOSFET, Modified feed forward.

## 1. Introduction

### *1.1 Physical Un-clonable Function*

As electronic devices have become increasingly interconnected in people's lives, security, trustworthy, and privacy protection have become a major goal of hardware design objective over the few past decades. In the olden days, secret keys are embedded into integrated circuits (ICs) in a ROM immediately after manufacturing. But digital keys stored in a non-volatile memory are vulnerable to physical attacks which often succumbs its originality to hackers. This attack on the integrated circuits dispute has become more intense recently, and the need for using intrinsic random features of physical objects or hardware for identification and authentication has become a need in order to protect the originality of the ICs. Thus, there is of need of PUFs in the silicon circuits.

Several types of PUFs exist. Some of the commonly used PUFs are multiplexer PUFs, ring oscillator PUFs and SRAM based PUFs. The faults or variation introduce during the fabrication process leads to the unique characteristic of these hardware circuits which is being extracted and utilized for providing a unique signature for the chip. Because of the wild arbitrary components, PUFs are easy to make however it is virtually difficult to clone, anticipate, or repeat. Moreover, it is infeasible for an attacker to plot an attack to forge the secret data without changing the physical randomness [Yingjie Lao and Keshab K. Parhi (2001 ),

S. V. SandeepAvvaru, Chen Zhou, Saroj Satapathy, Yingjie Lao, ChrisH. Kim, Keshab K. Parhi (2008),

Rahim Pegu,Rajkishur Mudoi(2015) ]. For instance taking coating PUF as an example, which is a function built on top of an IC layer by filling the space between and above the comb structure with a solid material and arbitrarily doping with dielectric materials. And by doing so in the top layer of an IC any attack on the physical entity would damage the protective coating thereby destroying the secret or unique key[Daihyun Lim, Jae W. Lee, Blaise Gassend, G. Edward Suh, Marten van Dijk, and Srinivas Devadas (2005)]. The general puf is given in Figure. 1.

### *1.2 Related Work and Our Contribution*

The first PUF is the optical PUF, where the randomness in the device is that of the position of the light scattering particles and the intricacy of the interaction between the light and the particles. After Optical PUF, several PUF hardware structures have been suggested. Most PUFs uses conventional silicon techniques so that any type of elaborate and special fabrication is not require and can be easily integrated into IC chips, except few types of PUF like magnetic PUF and coating PUF. Among these PUFs, silicon PUFs comes out to be the best choice as this type of PUF that exploits the manufacturing fickleness of wire delay to generate a unique challenge-response mapping of the integrated circuit. The objective of this paper is to design a different architecture low power linear and feed-forward arbiter PUF and compare it with the previous arbiter PUF shown in Figure. 2. The effect of the new architecture on the performance matrix of the PUF will also be discussed in this paper.

### *1.3 Paper Organization*

The rest of the paper is organized as follows. In Section 2, we introduce the background of silicon PUFs, and then present a brief overview of previous works on feed-forward PUFs. In Section 3, we describe our manufacturing process variation model for the feed forward PUFs and the experimental methods and demonstrate the parameters comparison by providing experimental results on TANNER EDA tool. Finally, concludes the paper.

## 2. Background

### *2.1 Silicon Physical Unclonable Function (PUF):*

Silicon PUFs exploit the delay difference of CMOS logic components to create a unique response for every IC. There are two fundamental delay-based silicon PUFs: Ring Oscillator (RO) PUF and Multiplexor (MUX) PUF. However, considering its degree of security against attackers the MUX PUF is considered more secure than the RO PUF, as the frequencies of the ring oscillators can be rather easily evaluated by the attackers. In addition to this, a MUXPUF is more suited for resource-restraint applications. Instead of replicating the hardware for N number of times as in a RO PUF, we can use N number of dissimilar challenges to obtain an N-bit long response in a MUX PUF [Jae W. Lee, Daihyun Lim, Blaise Gassend, G. Edward Suh; Marten van Dijk, and Srinivas Devadas (2014)]. This sort of silicon PUF comprises of N stages MUXs and one arbiter which connect the last stage of the two paths. The signal or the input when propagating through the PUF, the MUXs in each stage act as a switch to either cross or straight path propagating through the rising edge of the signal. Each MUX which comprises the PUF should be designed exactly the same, while the variations or the randomness in its physical properties will be introduced only during manufacturing process. Finally, the arbiter transfer the analog signal into a digital value in the form of either 1's or 0's.. For transistors, manufacturing randomness in transistors exists due to variations in channel length, width, gate oxide thickness, doping concentration density, metal width, metal thickness, and ILD (inter-level dielectric) thickness, etc. A vast amount of variation is introduced during the manufacturing variations that are sufficient enough to generate a secret and unique challenge-response pairs for each integrated-circuit by analyzing the two delay paths.

### *2.2 Feed-Forward Structure*

Because of the various attacks on linear PUF like linear modeling a feed-forward structure of silicon PUF has been suggested. The basic structure of feed-forward PUF is displayed in the following Figure.ure which uses the speeding respond of an intermediate stage as the select signal for a block of MUXs in the later stage[Y. Lao and K. K. Parhi,I(2011)] This structure gives nonlinearity to the original PUF, which expands the multifaceted nature for numerical modeling attacks. However, the reliability of the PUF has been diminished in this feed-forward structure as any sorts of error in the responds of an internal feed-forward arbiter generated by environmental variance can optimize the noise anticipation in the final response.

### *2.3 Performance matrix to be analysed*

#### *2.3.1 Reliability:*

Reliability defines how balance is the CRPs of the given PUF against different operating conditions. The dynamic operating conditions can be taken as the variations in temperature, supply voltage and ambient noise. The intra chip deviation is the unit of reliability of PUFs that is controlled by correlating the analog impression of the PUF as for similar test under various environmental conditions or temperature situation [R. Maes, P. Tuyls and I. Verbauwhede 2008), S. Nassif (2000), J. Guajardo, S. S. Kumar, G.-J. Schrijen, and P. Tuyls((2007)]. Here, we consider P$intra$ as the probability that a response of 1's at some point of time may flip when applied with a randomly selected challenge for a multiple number of times. Thus, P$intra$ may be utilized to serve as the intra chip dissimilarity for the whole response. The difference between the intra-variation response forms the hamming distance which is used for variation in MUX-based PUFs. The Pintra or the hamming distance (HD) average is defined as :

$$\text{Pintra} = \text{E}\left(\frac{1}{m}\sum_{i=1}^{m}\frac{HD(R,R^{'})}{L} \times 100\%\right) \qquad (1)$$

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:

$$\text{Reliability=1-Pintra} \qquad (2)$$

#### *2.3.2 Power:*

Power is one of the main parameters to be analyzed in a every device. As according to ohms law

$$P=VI \qquad (3)$$

So, in a DG MOSFET, VT as low as 0.1 V can be achieved as dynamic control of VT can be achieved. And as for the current is concerned, gate leakage current is prevented by a thick gate oxide and it provide better Ion/Ioff.

## 3. Methodology

### *3.1 PUF Model*

A standard MUX comprises of a series of N stage MUXs and an arbiter. The two arrays of the MUXs will be excited by the rising edge of the input signal. The actual path of procreation will be judged by the challenge bit applied externally. The arbiter circuit will generate the response depending on which rising edge of the two path arrives first. And respectively the response through the arbiter is either '0' or '1'.

In this paper, we are relying on simulation method for evaluating the power, intra variation and reliability of the PUFs instead of actual fabrication considering the many advantages it has upon fabrication. Some of the notable mention may be the expenses it saves and a reliable simulation can be employed as a pre-fabrication test. And above this we can foresee the efficiency of any proposed PUF and need not to mention the trend of following with the shrinking technology.

### *3.2 Power and reliability analysis of basic feed-forward MUX PUF.*

Here, we have taken a 14-stage basic feed-forward MUX PUF in 65nm technology and. Two clock signals of different frequency are provided to excite the two paths at the same time. The actual propagated paths will be determined by the external applied challenge bits. The said PUF is simulated at 0°C, 10°C, 25°C and 35°C at Tanner EDA tools. The simulated response is shown in the following waveform in Figure. 5.

### *3.3 Power and reliability analysis of the proposed feed-forward MUX PUF using DG MOSFET.*

### *3.3.1. Double Gate MOSFET*

As the single gate device at nano-scale has been suffering from short channel effect, the use of multi gate structures as shown in Figure. 6 have become quite important in today's silicon industries to overcome such problems [(Hon-Sum Philip Wong, David J. Frank, and Paul M. Solomon (1998)]. Among the multi gate MOSFET, DG might be the unique viable alternatives to build a nano MOSFET when channel length is lesser than 50nm.Better Ion/Ioff, improved sub-threshold slope, reduced Vdd, and reduce leakage current are some of the various advantages it has over the single gate MOSFETs.DGT is comprised of a drain, source, and two gates with conducting channel surrounded by gate electrodes on either side. It gives good control of the channel by the gate node. This guarantees none of the portion of the channel is far from a gate node. The electric field is controlled by the voltage applied at the gate terminals which determines the amount of current flow through the channel. The most common mode of operation is to switch both gates simultaneously. Another mode is to switch only one gate and apply a bias to the second gate. The Double Gate MOSFET minimizes the short channel effect which allows device downscaling more drastically up to 7 nm. The proposed circuit is designed using this device. The multiplexer and latch is shown in Figure.7 and 8 respectively.

### *3.3.2 Simulation of feed-forward MUX PUF using DG MOSFET.*

Here, we have taken 14-stage feed-forward MUX PUF in 45nm technology elaborated in Figure. 9. Two clock signals with different frequency provided will excite the two parallel paths simultaneously. The power is reduced by 99%. The reliability is increased by 0.7%. The area is reduced due lower technology. The actual propagated paths will be determined by the external applied challenge bits. The said PUF is simulated at -5°C, 0°C, 10°C and 25°C at Tanner EDA tools. The simulated response is shown in the following waveforms in Figure.10 and 11.

## 4. CONCLUSION AND FUTURE SCOPE

With the comparative presentation of the various MUX based PUF, the experimental result clearly reflects the characteristics of the two feed-forward PUF with respect to power and reliability. The average power consumed get relatively lesser on our proposed model and so with its reliability also. Table 2 shows a power comparison at different temperatures. But one major drawback is the range of temperature in which the proposed model can operate without affecting the reliability. The future work will be directed towards the evaluation of MUX-based PUFs from a temperature and reliability perspective through various types of modeling technique.

## References

Yingjie Lao and Keshab K. Parhi (2001 ), *Reconfigurable Architectures for Silicon Physical Unclonable Functions,*Yingjie Lao and Keshab K. ParhiDepartment of Electrical and Computer Engineering, University of Minnesota, Twin Cities.

S. V. SandeepAvvaru, Chen Zhou, SarojSatapathy, Yingjie Lao, ChrisH. Kim, Keshab K. Parhi (2008), *Estimating Delay Differences of Arbiter PUFs Using Silicon Data*, Department of Electrical and Computer Engineering University of Minnesota Minneapolis, MN 55455 USA.

Rahim Pegu, Rajkishur Mudoi(2015) ,*Design and Analysis of Mux-based Physical Unclonable Functions* ,International Journal of Engineering Research & Technology (IJERT), ISSN: 2278-0181, Vol. 4 Issue 05.

Daihyun Lim, Jae W. Lee, Blaise Gassend, G. Edward Suh, Marten van Dijk, and Srinivas Devadas (2005), Extracting Secret Keys From Integrated Circuits. ieee transactions on very large scale integration (vlsi) systems, vol. 13, no. 10.

Jae W. Lee, Daihyun Lim, Blaise Gassend, G. Edward Suh; Marten van Dijk, and Srinivas Devadas(2014), *A Technique to Build a Secret Key in Integrated Circuits forIdentification and Authentication Application*s, MIT Computer Science and Artificial Intelligence Lab (CSAIL) Cambridge, MA 02139.

Y. Lao and K. K. Parhi,I(2011),*Reconfigurable architectures for silicon physical unclonable functions,* in Proc. IEEE Int. Conf. Electro Inf. Technol., pp. 1–7.

R. Maes, P. Tuyls, and I. Verbauwhede(2008), *Statistical analysis of silicon PUF responses for device identification*, in Proc. SECSI Workshop.

S. Nassif(2000), *Delay variability: Sources, impact and trends*, in Solid-State Circuits Conference, pp. 368–369.

Hon-Sum Philip Wong, David J. Frank, and Paul M. Solomonm(1998), *Device Design Considerations for Double-Gate, Ground-Plane, and Single-Gated Ultra-Thin SO1 MOSFET's at the 25 nm Channel Length Generation*, IEEE IEDM , San Francisco,CA,p-407.

Table1: Comparison of simple feed-forward mux PUF and DG MOSFET feed-forward mux PUF

| Parameters | Existing | Proposed |
|---|---|---|
| Vdd | 1 | 0.5 |
| technology | 65nm | 45nm |
| Number of stages | 14 | 14 |
| area | Higher | Lower |
| No. of transistor | 224 | 244 |
| Intra variations | 1.5% | 0.78% |
| reliability | 98.5% | 99.22% |
| Power(at 25 c) | 52.2 uw | 2.5 uw |

Table2:Power of proposed circuit at different temp

| S. No. | Temperature | Power dissipation (uw) |
|---|---|---|
| 1. | -5 | 0.6 |
| 2. | 0 | 1.2 |
| 3. | 10 | 1.8 |
| 4. | 25 | 2.5 |

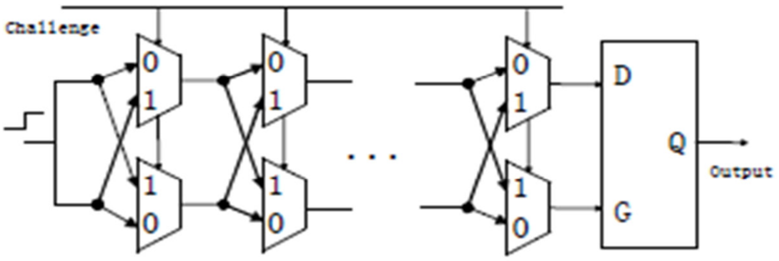

Figure1. General representation of PUF

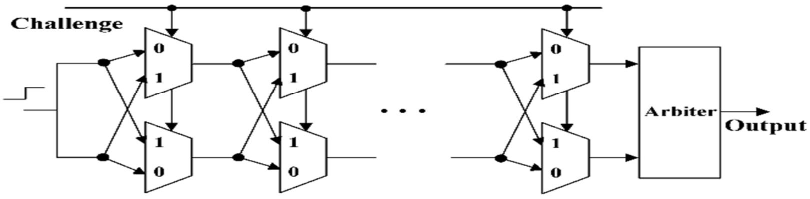

Figure 2. An arbiter based PUF structure

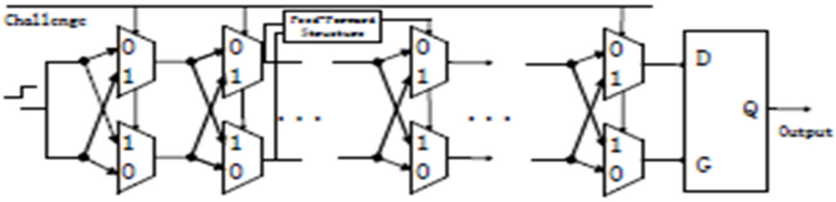

Figure3.Feed-forward silicon MUX PUF structure

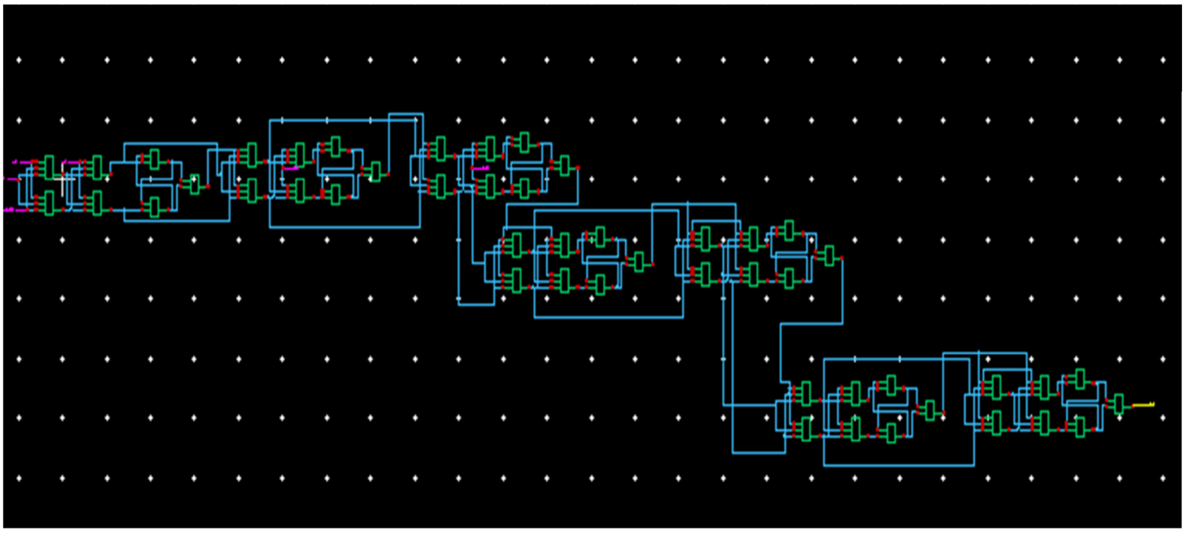

Figure 4.schematic diagram of 14 stage basic feed-forward MUX PUF

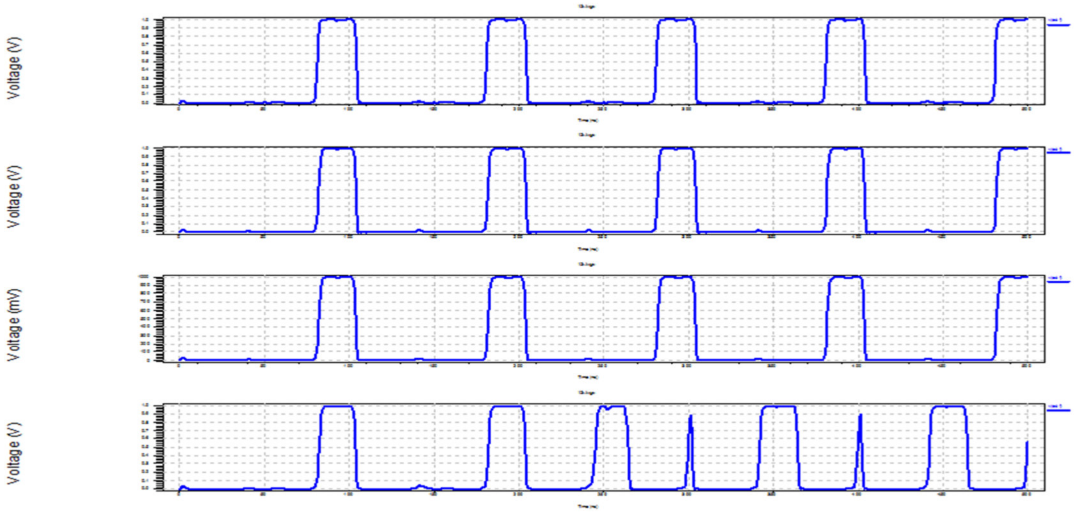

Figure5. Analog simulated output at 0°C, 10°C, 25°C and 35°C

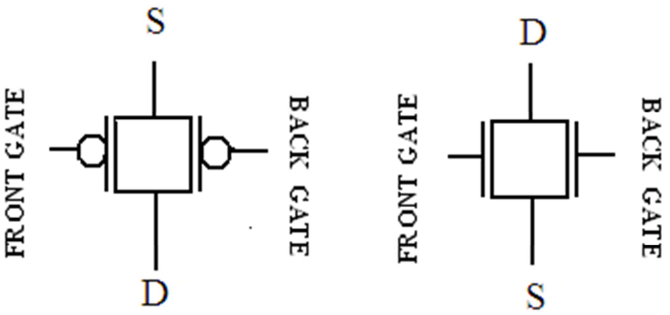

Figure6. DG MOSFET of pmos and nmos

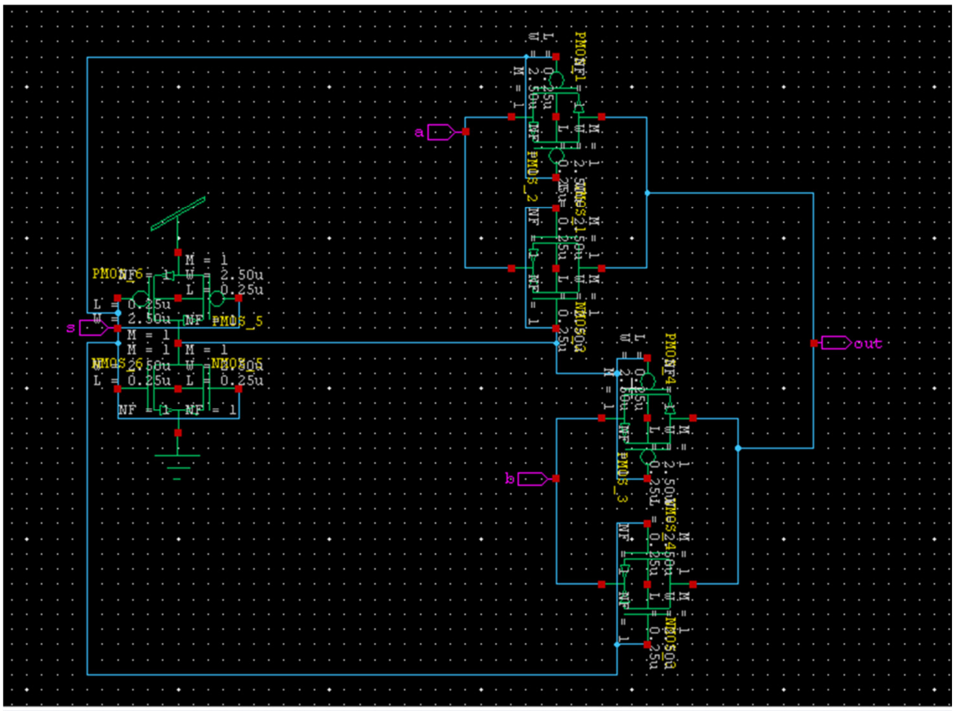

Figure7. MUX schematic using DG MOSFET

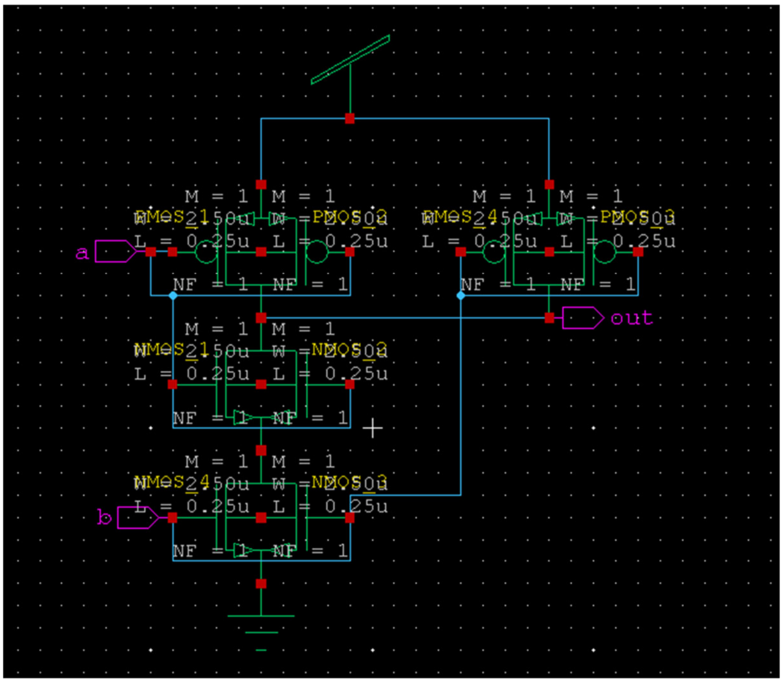

Figure8.Latch schematic using DG MOSFET

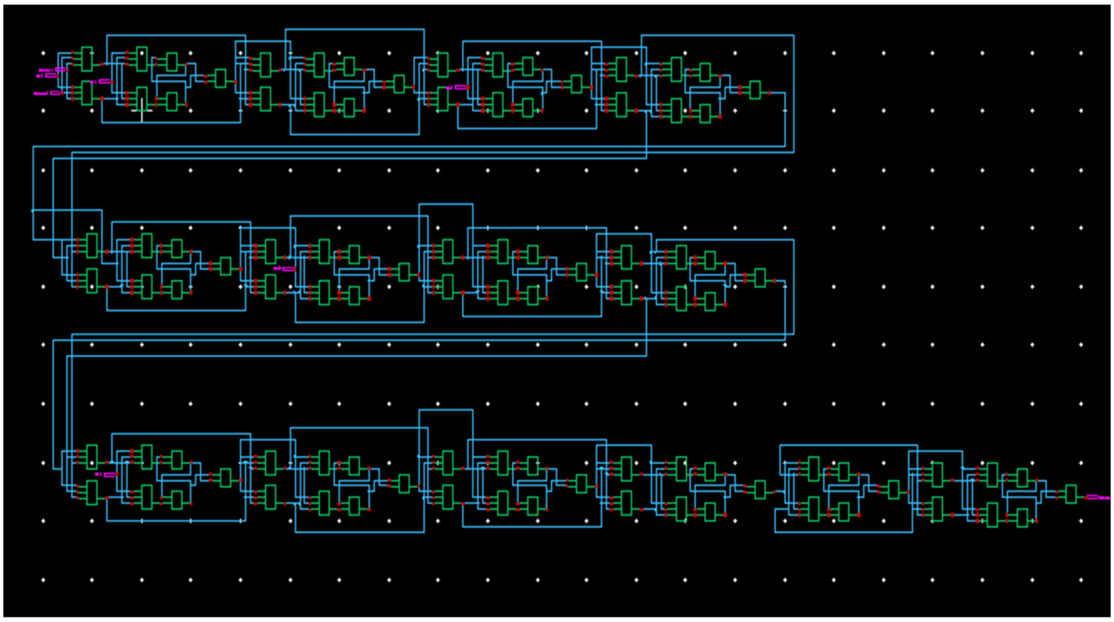

Figure9. Schematic diagram of 14 stage feed forward PUF using DG MOSFET

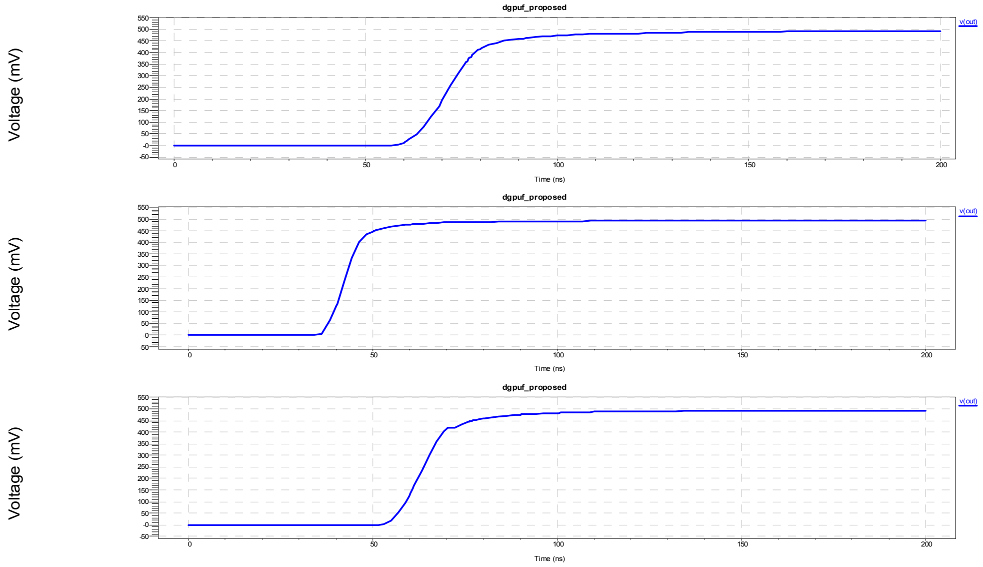

Figure10. Analog simulation output performed at -5°C, 0°C and 10°C

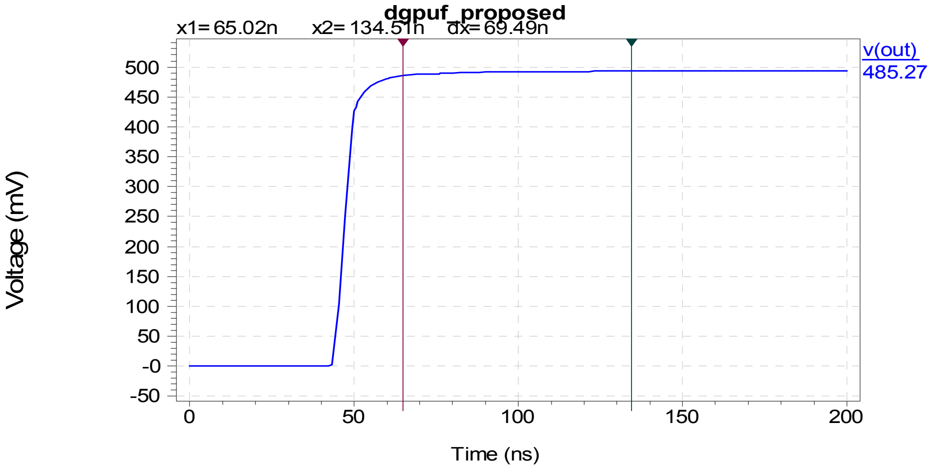

Figure11. Analog simulation output performed at -25°C