PHYSICAL UNCLOANABLE FUNCTION (PUF)

DISSERTATION II

Submitted
By

KONSAM JEMSON MEITEI
Department of ECE

In partial fulfilment of the Requirement For the

Award of the degree of

MASTER OF TECHNOLOGY
IN
VLSI DOMAIN

Under the Esteemed Guidance of

MR. JYOTIRMOY PATHAK

School of Electronics & Communication Engineering
Lovely Professional University, Punjab
MAY 2017

CERTIFICATE

This is to certify that the dissertation titled "**PHYSIVAL UNCLOANABLE FUNCTION(PUF)**" that is being submitted by "**KONSAM JEMSON MEITEI**" in partial fulfilment of the requirements for the award of **MASTER OF TECHNOLOGY DEGREE (VLSI)**, is a record of bonafide work done under my guidance. The content of this report, in full or in parts, have neither taken from any other source nor have been submitted to any other Institute or university for award of any degree or diploma and the same is certified.

Mr. JYOTIRMOY PATHAK
ASSISTANT PROFESSOR
(LOVELY PROFESSIONAL UNIVERSITY)

Objective of the Thesis is satisfactory /unsatisfactory

Examiner I **Examiner II**

ACKNOWLEDGEMENT

I would like to thank **LOVELY PROFESSIONAL UNIVERSITY** for giving me opportunity to use their resource and work in such a challenging environment. I am grateful to the individuals whom contributed their valuable time towards my thesis.

I wish to express my sincere and heart full gratitude to my guide "**MR JYOTIRMOY PATHAK**" Assistant professor, who guides me to take up this thesis in sync with global trends in scientific approach.

I would also like to extend my gratitude to my friends and family who always encouraged and supported me in this thesis work.

KONSAM JEMSON MEITEI
Reg. No. 11508694

DECLARATION

I, **KONSAM JEMSON MEITEI,** student of **MASTER OF TECHNOLOGY (VLSI)** under Department of ELECTRONICS ENGINEERING of Lovely Professional University, Punjab, hereby declare that all the information furnished in this dissertation-II report is based on my own intensive research and is genuine.

This dissertation-II, to the best of my knowledge, does not contain any part of my work which has been submitted for the award of my degree without proper citation.

Date:

KONSAM JEMSON MEITEI
Reg. No. 11508694

LIST OF CONTENTS

LIST OF FIGURES

LISTS OF TABLES

ABSTRACT

Physical Unclonable Function (PUF) is a physical entity that provides secret key or fingerprints in silicon circuits by exploiting the uncontrollable randomness during its manufacturing randomness. Its provides a hardware unique signature or identification. Its properties 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 were quantified by the inter-chip variations, intra-chip variations and reconfigurability 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 analysed its parameters like reliability and power.

INDIA'S LARGEST UNIVERSITY
LOVELY PROFESSIONAL UNIVERSITY
Transforming Education, Transforming India

TOPIC APPROVAL PERFORMA

School of Electronics and Electrical Engineering

Program : P175::M.Tech. (Electronics and Communication Engineering) [Full Time]

COURSE CODE : ECE521 **REGULAR/BACKLOG :** Regular **GROUP NUMBER :** EEERGD0216

Supervisor Name : Jyotirmoy Pathak **UID :** 16082 **Designation :** Assistant Professor

Qualification : ________________________ **Research Experience :** ________________________

SR.NO.	NAME OF STUDENT	REGISTRATION NO	BATCH	SECTION	CONTACT NUMBER
1	Konsam Jemson Meitei	11508694	2015	E1514	9915122907

SPECIALIZATION AREA : VLSI Design **Supervisor Signature:** ___________________

PROPOSED TOPIC : Design of a Physically Unclonable Function for generation of random sequence for hardware security.

Qualitative Assessment of Proposed Topic by PAC		
Sr.No.	**Parameter**	**Rating (out of 10)**
1	Project Novelty: Potential of the project to create new knowledge	7.67
2	Project Feasibility: Project can be timely carried out in-house with low-cost and available resources in the University by the students.	8.00
3	Project Academic Inputs: Project topic is relevant and makes extensive use of academic inputs in UG program and serves as a culminating effort for core study area of the degree program.	8.00
4	Project Supervision: Project supervisor’s is technically competent to guide students, resolve any issues, and impart necessary skills.	8.00
5	Social Applicability: Project work intends to solve a practical problem.	8.00
6	Future Scope: Project has potential to become basis of future research work, publication or patent.	8.00

PAC Committee Members		
PAC Member 1 Name: Anshul Mahajan	UID: 11495	Recommended (Y/N): Yes
PAC Member 2 Name: Dushyant Kumar Singh	UID: 13367	Recommended (Y/N): NA
PAC Member 3 Name: Cherry Bhargava	UID: 12047	Recommended (Y/N): Yes
PAC Member 4 Name: Anshul Mahajan	UID: 11495	Recommended (Y/N): Yes
DAA Nominee Name: Manie Kansal	UID: 15692	Recommended (Y/N): NA

Final Topic Approved by PAC: **Design of a Physically Unclonable Function for generation of random sequence for hardware security.**

Overall Remarks: Approved

PAC CHAIRPERSON Name: 11211::Prof. Bhupinder Verma **Approval Date:** 08 Oct 2016

4/28/2017 3:43:39 PM

CHAPTER 1

INTRODUCTION

1.1 HISTORICAL OVERVIEW

Reference of exploiting the hardware properties of systems for verification purposes dates back to the early 1980's. An authentication scheme for memory cards was provided by Naccache and Fremanteau in 1992. By the early 2000's the terem physical one way function(POWF) and physical unclonable function were composed. To be more specific in 2001 and 2002 respectively. PUF gained its attention in the smartcard market from 2010 till 2013 as a unique way of providing "silicon unique identity".

1.2 ATTACKS ON IC CIRCUIT

The advancement of semiconductor device has altered the world and empowered numerous incredible applications. For instance, the cell phones and tablets have now turned out to be so predominantly utilized as a part of online instalment, web program, gaming, individual information aide and individual human services than the standard elements of its antecedent component telephones and PCs. The every inescapable impact of electronic gadgets can be felt in each part of our present life. The propeller behind this ever quicker reestablishment of electronic devices is the interminable increment in gadget coordination thickness is the increase in device integration density (the quantity of gadgets per unit range in a coordinated circuit (IC)) anticipated by the Moore's Law in the "silicon era".

The significantly increase in the intellectual and authoritative complexity of IC configuration is driving the semiconductor enterprises towards a vertical specialization where different phases of IC configuration are broken down, outsourced to outside firms also, moved crosswise over national limits that have the implied information and skill. For the most part, the design of an IC is encouraged by the following outside administration and resource providers:

- Electronic design automation(EDA) organizations give the intense and complicated programming instruments that guide the design and confirmation of present day ICs.

- Semiconductor foundries furnish the IC design with the electronic gadget models and the administrations to create and fabricate the chips with their own resource so that the creators can profit by the lower per capital cost of chip assembling and center their innovative work exertion on the item works required by the end markets**.**

- Cell library engineers and Intellectual property (IP) center sellers give the IP blocks, for example, the standard and particular cell libraries, CPU centers, memory and controllers that have been completely tried and streamlined to convey the coveted execution. These IP block help to decrease the outline time, enhance the quality and yield, and meet the brief timeframe to-market window for the advancement of the unpredictable framework on-chip.

- The dynamic interest of the different outside specialists in the outline and assembling stream of an IC has made the whole IC store network exceptionally defenseless to chip corruption and subversion. Thus modern ICs have been under various threats in the design and fabrication procedure. Some of the mainstream examples of such threats in the different stages of IC design procedures are given below:

- Malignant logics (hardware Trojan) insertion: The original design can be altered in the deaign stage or amid the manufacture stage, if the enemy picks up the entrance to it. The equipment Trojans may conceivably release the delicate information, lessen the IC dependability or make a framework come up short at a basic time. The Trojans for the most part don't change the first function of the circuit and furthermore very little in size, which can barely be recognized by the parametric tests performed by the real users

- IP theft: The hacker can break down the plan or take the IP. The stolen IP can be unlawfully utilized or replicated to mass create or fake the plan. After effects of the investigation on the stolen IP can likewise be utilized by plotting aggressors to help in future programming or equipment construction.

- Reverse engineering : High-class ehackers can spend days getting to the chip surface straightforwardly and watch the IC layout layer by layer with the help assistance of the current equipments. These intrusive attack can help the hackers comprehend the inner components and structures of the outline. With this data, the hackers can undoubtedly fake the plan, and embed pernicious equipment Trojan to sidestep identification or take the sensitive information stored in the IC.

- Fault injection: The equipment Trojans or the secondary DOOR implanted in an IC can be activated by presenting it to abnormal working conditions (concentrated light pulse, radiation, and so forth.).

- Side-channel attack : This attack depends on data picked up from the physical usage of a crypto-framework, as opposed to by brutal constrain or through misusing hypothetical shortcomings in the cryptographic calculations. The side-channels of a gadget can be the delay, control utilization or the electronic attractive radiation.

The fast developing complexity of ICs and the dependence on outsourcing of schedule and the less important value included in the IC value chain have made guaranteeing the IC trustworthiness more troublesome than any other time in recent memory. In the mean time, present day and rising innovations, for example, filtering optical microscopy, light incited voltage shift and machine learning, are likewise making it simpler to attack an IC after its organization.

As opposed to the approaching CMOS gadget scaling anticipated many years ago, technology scaling ends up being a key empowering agent of hardware cryptography. Security primitives have been incorporated with lightweight applications that would have been unbelievable only 10 years back. In 2005, the Defence Advanced Research Projects Agency (DARPA) starts the Trust in ICs program. From that point on, persistent developments have been brought into this incipient field. With Internet of Things (IoT) conceived to wind up plainly an extreme driver for the following development period of semiconductor industry, Radio frequency identification (RFID) and a few other lightweight electronic labelling advancements will benefit themselves most in this universal figuring upheaval of progress network of gadgets, frameworks and administrations. unfortunately, the impression and control spending plan have seriously constrained the quality of cryptographic calculation implementable on a RFID or other intelligent labels, and the mystery information put away in these lightweight gadgets can be effortlessly perused or figured out and duplicated.

Critics are worried that the image of IoT will make digital attack an inexorably annihilating physical (instead of virtual) attack. Another reason that makes hardware security an appealing examination zone is that it is the last line of protection. Software security has been tormented by security issues for a long time, and hardware has for quite some time been touted as a place of boon for security insurance. All in all, hardware oriented security has the accompanying two special focal points over the software based security:

- Minimal operation level: The operation of the hardware is situated in the least level. Hardware security primitives can be quicker, exceptionally application-particular what's more, more productive than the software instruments. Moreover, programming security measures can do little against some capable equipment assaults, for instance, micro probing.
- Modifiability: The capacity to effectively change or refresh the product is a ambiguous tool. On one hand, this can help the developers settle and fix known software bugs rapidly. Then again, a similar adaptability can likewise be misused by the aggressors to introduce infections or Trojans in the working framework. Interestingly, the inserted secure equipment circuits in a chip can't be effectively altered after the IC deployment.

Nevertheless, without adequate protection, any hardware can be as vulnerable as the software. Any successful attacks to a hardware integrated system can cause greater disruptions, leading to heavier economic losses and may even endanger human lives. Given the tight coupling between information and communication technologies and physical systems today, the new security concerns of disastrous hardware attacks are requiring a rethinking and re-examination of the commonly used objectives and methods.

1.3 HARDWARE SECURITY OR PUF

PUFs is a hardware peripheral that is represented in a hardware system and is anything but difficult to assess however difficult to anticipate. More than that, an exclusive PUF hardware or gadget have to be anything but difficult to build however in every way that really matters hard to duplicate, even given the right gathering process that made it. The name PUF may be small beguiling as few of them are might still be duplicated, and almost all of them are clamorous and in this way don't fulfill the necessities of a function.

Now a days , PUFs are realised in IC and are regularly used as a piece of components with high security necessities. It is a input to output framework in which the mapping between a input and the output is subjected to the variation in properties of a physical material. For example, an on-chip PUF is a chip-special test reaction framework misusing the manufacturing procedure assortment inside IC. The association among an input and its output is directed by confounding, quantifiable assortment in method of reasoning and adjoining in an IC. A PUF is essentially a fluctuation mindful circuit which can perceive the mismatch in circuit parts made by collecting process variety.

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 concludes that each and every PUF have a different identification like fingerprint as of human being. The PUF is embedded in physical device in an inseparable way for secure identification of the device to be identified. Due to the fractious random component, PUFs are not hard to measure but hard to copy, conclude or recreate practically. Moreover, they are impossible to mount an invasive attack which will copy the classified data without interrupting physical unpredictability. Because of such advantages, in cryptographic application, PUFs can be applied for generation of efficient and reliable secret key; and enables low cost authentication of ICs (Integrated Circuits).

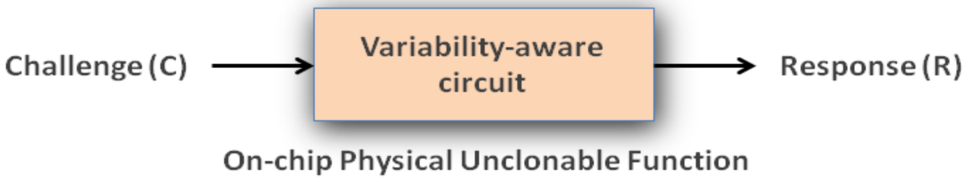
Challenge (C)
Variability-aware circuit
Response (R)
On-chip Physical Unclonable Function

Fig1: General representation of PUF

1.4 Types of Silicon PUF

In the course of the most recent few years, numerous number of PUFs have been effectively proposed for the security applications because of the promising properties of physical unclonability, alter proof and little equipment overhead. This survey centers on the most well known silicon based PUFs, as they are easy to be coordinated with the standard CMOS process. generally, there are two essential applicatins of PUFs: authentication and secure key generation. In view of the two applications, the PUFs are extensively sorted as "strong PUFs" and "weak PUFs". Strong PUFs can be focused for authentication, while weak PUFs are more reasonable for the secret key generation.

Prior to the examination of the classifications and operations of the PUFs, the terminologies for PUF are presented. The input and output of PUFS circuits are ordinarily called as the challenge and response. A given challenge and its respectiveresponse are termed as challenge response pair(CRP). Actually, the crucial contrast between the WEAK and solid PUFs lies in the connection between their challenge and response.

1.4.1 Strong PUF

Strong PUFs are cluttered physical systems with a complex challenge-response behaviour characterized by a substantial challenge-response space. It is virtually impossible to clone a strong with the same CRPs as that of the original PUF. And furthermore, measuring or determining all the specific CRPs for a strong PUFs is impossible for an attacker within a limited time. The main examples for the strong PUFs are: the arbiter delay PUF and the ring oscillator (RO) PUF.

- **Arbiter PUF**

In the arbiter PUF, a symmetric circuit is taken a race condition is establish by giving different challenges. Fig. below shows the implementation of the basic arbiter PUF. It consists of a string of switches, of which each switch is controlled by one bit of the challenge. When an input is given, at the beginning the rising edge is split into the two multiplexors. Different path are being selected by the different input challenges. Because of the variation in the manufacturing process in the gate delay of each stage one edge will arrive at the latch faster than the other even though the two channel or the selected two lines are laid out in the same fashion. The arbiter circuit or here latch will processed whichever edge arrives firt of the two string thereby producing the response. So it can be concluded that the response is determined by the challenge bits

It can be noticed due to the metastability of the arbiter makes the PUFs prone to environmental noises. Furthermore, the digital delay in the basic arbiter PUF has to be considered. In other words, the delay of each array of switch blocks is the sum of the delay in each stages. This can makes the arbiter PUF susceptible to the model-building attacks. By observing a number of CRPs, one might be able to build a mathematical model that predicts the response of future challenge that might be of high precision. There are a couple of adjusted architecture proposed which might overcome model-building, by presenting nonlinearity in the delays and by limiting the I/Os to the PUF.

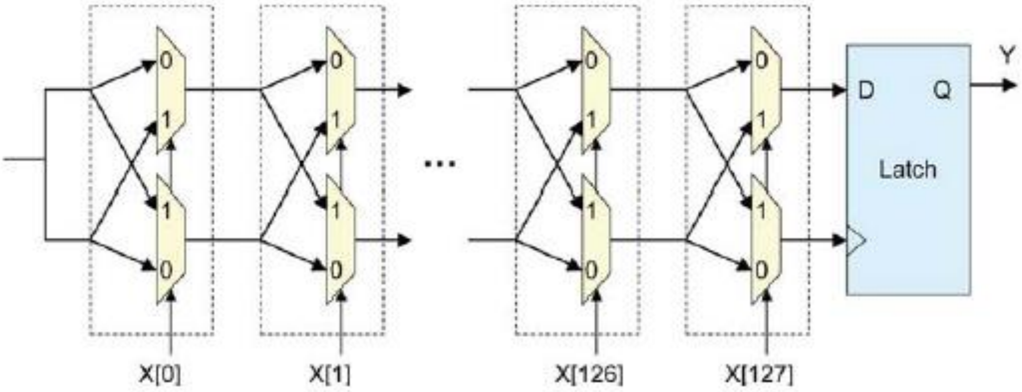

Figure 2 : The schematic of arbiter PUF

- **(RO-PUF)- Ring Oscillator PUF**

The simple RO PUFs architecture comprises of 2N-1 multiplexors, dual counters, single comparator and N similar ring oscillators, as shown in figure. An odd number of inverters in a feedback loop comprises each ROs. The delay in the inverter array in each RO differs Due to the inter- and intra-chip process variations and environmental variability, which might make a deviation of the oscillation frequencies between any two ROs. The data select lines of the two multiplexors is fed with a 2log2N-bit challenge to elect a pair of ROs. The output frequencies of the elected ROs are then used to clock two similar counters. A comparator is then connected with the two counter outputs. The output bit of the PUF which is the counter output, is either 0 or 1 depending on which oscillator has reached the same pre-loaded count value earlier. So, the difference between the oscillation frequencies of any RO pair, the output r bit of the PUF is more reliable. RO PUFs have more physically strong to layout differences.

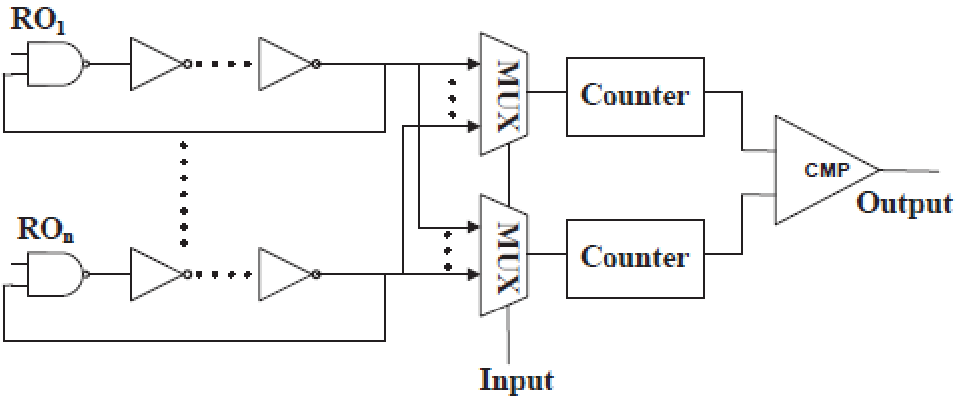

Figure 3: Simple ring oscillator puf architecture

1.4.2 Weak PUF

Rather than the solid PUFs, the weak PUFs may have less CRPs. Weak PUFs can normally viewed as a unique type of memory, yet they are more strong to the intrusive attack than the non-volatile memory like EEPROM. The most mentioned weak PUFs are the memory-based PUFs: SRAM PUF, latch PUF and butterfly PUF.

- **SRAM PUF**

SRAM is a notable weak PUF structure that endeavors the positive feedback loop in a SRAM cell. As shown in the figure below it has two stable states: either "1" or '0'. The positive feedback in the cell compels it into one of these two states. When it enters either state, it averts the cell from traveling out of this state accidentally. In reference to the format, the double cross-coupled inverters are well proportioned as shown in the figure. It ought to be in the meta-stable state amid the charging stage. Be that as it may, in the genuine implementation, the circuit in the cross-coupled inverters are confounded due to the assembling process varieties. One of the feedback is somewhat more stronger than the other. The positive feedback of the cross-coupled inverters will be opened up by the mismatches and will in the long run produce either a logic 1 or a logic 0. Expecting irregular hardware variations, each SRAM cell may likewise create either logic 1 or logic 0 randomly with an equivalent probability of 50%. This makes the binary response string read out from the SRAM string one of a kind, arbitrary and non-traceable. Be that as it may, arbitrary noise, e.g., thermal noise and shot noise, can likewise trigger the positive feedback loop when it is in the meta-stable state, which makes the response of a SRAM PUF unstable. It is noticed that the last state relies on upon the contrast between two feedback loops. The estimation is taken differentially so that the impacts of common mode noise, for example, temperature, power supply vacillations, and common mode process variation will be reduced.

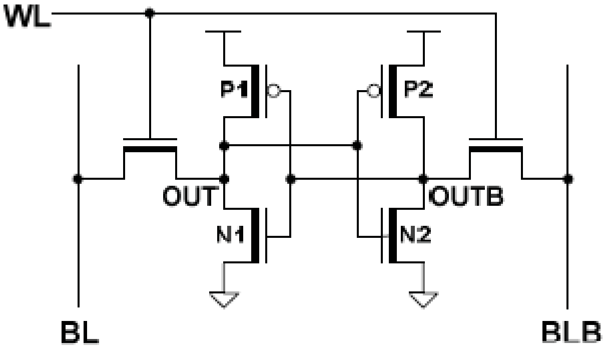

Figure 4 : simple structure of SRAM cell

- **Latch PUF**

Not every ICs have an SRAM array and it is difficult to just reset the SRAM subsequent after powering up for a few design. thus, the utilization of the SRAM PUFs is limited. Latch PUF was proposed to swamped the shortcomes of SRAM PUF. The logical structure of a latch PUF cell is shown in the figure below. Rather than cross-coupling two inverters in a SRAM cell, two NOR gates are cross-coupled. Like the SRAM PUF, by declaring a reset signal, this latch becomes uncertain and after that joins to a steady state again relying upon the internal difference between the electronic segments.

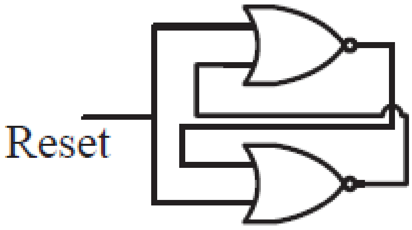

Figure 5: the logical structure of the latch puf cell

1.5 PUF APPLICATIONS IN HARDWARE SECURITY

Silicon PUFs are for the mostly intended for two applications in hardware security: device authentication and identification, and key generation for encryption units.

1.5.1 AUTHENTICATION AND IDENTIFICATION

PUF can be utilized to authenticate or confirm each ICs without utilizing costly cryptographic modules. This kind of validation is extremely helpful for resource obliged RFIDs where cryptographic operations are too costly as far as silicon range and power utilization. The validation or authentication with PUF utilizes a challenge-response protocol. After producing a gadget, the client of the PUF needs to keep the CRPs of its PUF in an enlistment stage. These CRPs are stored in a secure database. At the point when the ID or the validation is questioned, the challenges chosen from the enlistment stage are connected with the exact PUF. Since each PUF gives a novel reaction and its output must be calculated if one among them has the physical gadget, the confirmation is viewed as effective when the response matches (or sufficiently close to) the recorded one. To maintain a strategic distance from replay (spying) assaults, the used challenge ought not be used again. Consequently, it is greatly helpful to have a (strong) PUF that can support countless CRPs. This validation and authentication procedure can likewise be utilized by IC merchants to prevent forging attacks.

1.5.2 Key Generation

The security of a cryptographic framework depends not on the mystery of its calculation but rather in the mystery of its encryption and decryption keys. Generally, the keys are put away in non-volatile memory of a device which are powerless to obtrusive attack. Be that as it may, if a PUF's reaction to a special challenge (or some subsidiary of its response) is utilized as an encryption key, then the key is physically inserted in the device structure instead of put away in memory. Any intrusive or semi-obtrusive attack will definitely demolish the physical structure. So, the first information or the original data will never again be the same after the attack. It is also noticed that the response of a given PUF can't be utilized specifically as a key in cryptographic calculations, since its response are probably going to be distinctive in every assessment notwithstanding for the same challenge, and the raw response may not be really arbitrary. These constraints can be overcome by joining extra post-processing modules, for example, the error correction coder (ECC) or the fuzzy extractor. There are two stages in the error correction process: initialization and re-generation. In the initialization step, an error disorder is registered when the test is connected. This disorder is utilized later amid re-generated to rectify any errors that may have occured in the PUF response. The revised PUF response is then taken through a hash function to produce the unique key.

The alluring security applications for PUFs have likewise attracted the consideration industry by Verayo and Intrinsic ID. Verayo gives the PUF item as an IP to be authorized for RFID, ASIC and FPGA applications. Intrinsic ID offers secure key stockpiling solutions for protecting semiconductor items from cloning and reverse engineering

1.6 PUF Qualities and Metrics

There are three most important properties to consider while examining the quality of a PUF design, which are uniqueness, reliability and unpredictability. They are briefly explained as in the following paragraph:

- **RELAIBILITY:**

Reliability defines how balance are 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. 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. Difference between the intra-variation response forms the hamming distance which is used for variation in MUX-based PUFs. The P_{intra} or the hamming distance (HD) average is defined as :

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

Where, m= the number of HD comparisons
,R and R'= two measurements of the PUF output under different environmental state

Now with this in hand reliability of a PUF system can be defined as:

$$\text{Reliability} = 1\text{-P}_{\text{intra}}$$

- **Uniqueness:**

The inter chip abnormality is the measure of rareness that is assessed by looking at the hamming distance between two analog impression which are created from the same input and arrange information from various chips. We can characterize P_{inter} as the output created by a similar test for diverse PUF are distinctive. Since rareness is the unit for P_{inter} execution, almost all chip blends ought to be studied. Uniqueness can be measured by the medocre inter-chip Hamming Distance of the output produced by different PUFs.

Thus, the average P_{inter} of Z STAGES PUFs can be measured as:

$$\text{E(Pinter)} = \text{Pinter} = \text{E}(\frac{2}{Z(Z-1)} \sum_{I=1}^{K-1} \sum_{J=i+1}^{Z} \frac{E(R(i),R(j))}{L} \times 100\%)$$

- **RANDOMNESS:**

A PUFs may be utilized to stock clasified and coded keys, PUF response ought to be unusual/irregular with various known CRPs so as to guarantee that the classified information stays safe. A few measures of unconventionality have been used in the writing. As high accuracy more than 90% can be accomplished through machining learning attacks on direct PUFs, for example, Arbiter PUFs, one specially appointed measure of eccentrics is by deciding how appropriate machine learning assaults may be utilized as display CRPs of PUF. A MUX PUF is relied upon in a perfect world to deliver neutral 0's and 1's. Irregularity in the response represents the capacity of the PUF to yield 0’s and 1’s output with same probability. One estimation of of irregularity may be inclined as::

$$\text{Randomness} = 1 - |2 \times (R = 1) - 1|$$

When P(R = 1) is all the nearer to 0.5 it shows better randomness.

CHAPTER 2

LITERATURE REVIEW

The chapter is focused on review of literature of different fast adder designs. To conclude this topic many journals, articles, conference papers have been studied. Some of them are described as below.

- **S. V. SANDEEPAVVARU, CHEN ZHOU, SAROJSATAPATHY, YINGJIE LAO, C. H. KIM, K. K. PARHI (2016):**

Evaluating delay differences of each phase in a standard MUX-based physical unclonable capacity (PUF). Test information gathered from PUFs created utilizing 32 **nm** processes are utilized to prepare a linear model. The delay differences of the phase are directly corresponding to the model parameters. These parameters are prepared by utilizing an east mean square (LMS) adaptive algorithm. The correctness of the response utilizing the proposed model is around 97.5% and 99.5% for two dissimilar PUFs. Second, the PUF is likewise displayed by a perceptron. The perceptron has just about 100% classification correctness. These demonstrate shows that the perceptron model parameters are scaled versions of the model derived by the LMS algorithm. So, the delays differences can be evaluated from the perceptron demonstrate where the scaling component is registered by looking at the models of the LMS calculation and the perceptron. Because of the defer contrasts is test autonomous, these parameters can be put away on the server. So that, this will empower the server to issue random challenges whose responses require not be put away. Accordingly this examination demonstrates affirms that the delay differences of all phases of the PUFs on a similar chip have a place with the same Gaussian probability density function.

- **YINGJIE LAO, K. K. PARHI:**

PUFs are original device primitives that hold the unique data in silicon circuits by abusing uncontrollable arbitrariness because of assembling procedure varieties. In this case, it has as of now been demonstrated that a rearrangeable architecture of PUF won't just empower

PUFs to meet useful application needs, additionally can enhance the reliability quality and insurance of PUF-based verification or distinguishing system. Here , we proposed a few original structures of non-FPGA reconfigurable silicon PUFs, which needn't bother with any exceptional fabrication means and can conquer the confinements and disadvantages of FPGA-based methods. Their achievement are evaluated by the P_{inter} variation, P_{inter} variation and reconstructable tests. The delay-based silicon PUFs is constantly considered a stable input-output behavior and the PUF create equal or flaw tolerated output. These examination show that these PUF construction are powerless against a few attack techniques together with emulation, rerun, and reverse engineering. Also, updatable cryptographic keys are exceptionally fascinating in a few applications. Accordingly, a dynamic PUF which can modify the CRP each time the information is modified to keep the secret data spilled out is desired.

- **T.Addabbo, A.Fort, M.Mugnaini, S.Rocchi, V.Vignoli (2012):**

Silicon PUFs are innovative circuit primitives whose computerized yield altogether depend on upon the produce irregular physical assortments introduced in the midst of the fabricate strategy of coordinated circuits. The measurable portrayal of a basic PUF module depends on ring oscillators to actualize challenge-reaction FPGA validation. The test bits assume a part in changing the time flow required in the chip reaction estimation. The exploratory outcomes likewise demonstrate that by considering legitimate qualities for the test bits the repeatability mistake rate is littler than 5% at given chip temperature and supply voltage, getting a PUF module working with 4 challenge bits while showing a high affectability to the fabricate irregular physical varieties. The outcomes are practically identical to that one's exhibited for different arrangements, with a constrained utilization of equipment assets. For the most part, the arrangements misuse the wild wire deferral and voltage exchange attributes of straightforward computerized circuit primitives.

- **MUSLIM MUSTAPA, MOHAMMED NIAMAT (2014):**

Physical Unclonable Function (PUF) is a function that can't be demonstrated in light of the fact that it uses the random procedure variations from a silicon chip to produce a special piece stream of '1's and '0's (reaction bits) which can be utilized for verification/ authentication and cryptography applications. Furthermore, PUF is profoundly depend upon process varieties, the response bits created are represented by the efficient/ systematic procedure variation rather than the stochastic procedure variation, which will diminish the randomness in the response bits. The novel Random Patch Mixer (RPM) method is to reject the systematic variation effect on the response bits produced. RPM method is connected on information or information acquired from 29 Spartan 3E FPGA chips. These exhibit that the RPM technique has successfully ousted the orderly variety impact on the reaction bits created from the ROPUF on FPGA. These also exhibited that the reactions created by applying the RPM Technique passed the National Institute of Standards and Technology NIST measurable test for irregularity. ROPUF presents the time of '1's and '0's bit stream in view of the technique minor departure from a silicon chip. The method variety is a sporadic technique that occurs amid silicon chip creation brought on by the mistake in the manufacture methodology. The incorrectness brought on a little defer that is not useful operation of the circuit on a silicon chip. The ROPUF intensifies this little postponement through the recurrence era from a Ring Oscillator (RO). The qualifications in the frequencies delivered by the ROs will be used to make an arbitrary paired piece stream, which then can be used as the affirmation/confirmation or the cryptography encryption and interpreting key. The irregular double piece stream is known as a reaction. Each reaction is made by a given test from the customer or client. Test is a double piece stream that will choose the RO combine examination. Each test will convey a novel or one of a kind reaction. As ROPUF uses the technique assortments to make the secured reaction bits, there is so far a shortcoming exist since the think assortment governed the general system assortments. So it is basic to dismiss the consider assortment effect and augmentation the genuine irregularity on the reaction era in ROPUF.

- **TENGXU, DONGFANG LI, AND MIODRAGPOTKONJAK:**

PUFs are difficult to anticipate and difficult to imitate. Though, the utilization analytical models are to alterably describe the delay based PUFs, and utilize it as a starting stage to copy a delay-based PUF. The fundamental thought is that as for any input CA of a delay-based PUF A, there is a strong risk of finding a paired input CB. At the point when apply CB to another delay-based PUF B, it can deliver same output from applying CA on PUF A. These model outcomes demonstrate over 99% accuracy for the PUF response expectation utilizing characterization and 96% accuracy utilizing copying. Additionally tested the feasibility on the Xilinx Spartan-6 Field Programmable Gate Array (FPGA).

- **YINGJIE LAO, K. K. PARHI:**

PUFs has the ability hold classified keys in ICs by abusing the uncontrollable unpredictability because of assembling procedure variations. These PUFs can be utilized for verification or authentication of devicws and for key generation in security applications. This analysis presents a thorough statistical examination of different sorts of multiplexer-based (MUX-based) PUFs including the original MUX PUF, the feed forward MUX PUFs, the altered feed-forward MUX PUFs, and multiplexer-demultiplexer (MUX/DeMUX) PUF.
The altered feed-forward MUX PUF structure is new structure and three categories of feed-forward PUFs are studied in the paper. Those are listed below:

- Feed forward
- Feed forward cascade and
- Feed forward separate

The execution examination assesses between chip and intra-chip assortments as a component of the amount of stages; the system variety vacillation, the ecological clamor difference, and the referee skew for various PUFs. Three distinct estimations of execution are also introduced and analyzed in this paper, which consolidate dependability, uniqueness, and irregularity. A PUF will be more tried and true if there is less intra-chip variety. A PUF is more uncommon if the entomb chip assortment is more like half. A PUF is more arbitrary if its reaction bit is 0 or 1 with comparable likelihood. These factual examination shows that the intra-chip variety is less subject to the amount of stages, N, if N is more noteworthy than ten. Yet, the between chip variety is dependent on N if N is under 100. It is exhibited that the sustain forward PUFs have higher intra-chip variety than MUX PUFs, regardless, the nourish forward PUFs have fundamentally bring down intra-chip variety than the bolster forward PUFs. This likewise exhibited the changed - forward course MUX PUF has the best peculiarity and capriciousness, though there is greater unwavering quality in the primary MUX. The examination presented in this paper can be used by the initiator to pick PUF has a legitimate PUF in base on the application's need. This expels the require for creation and testing of various PUFs for picking a reasonable PUF.

- **MIAOQING HUANG AND SHIMING LI**

For hardware-oriented security point of view, Physically unclonable capacities (PUFs) have been a hot research point for a long time. Certain test has been given to the PUF as input, it creates a relating reaction, which can be dealt with as an extraordinary unique finger impression or mark for verification or authentication reason. Here, a delay-based PUF configuration including multiplexers in light of FPGA is introduced. Because of the characteristic contrast of the switching latencies of two chained multiplexers, a positive pulse might be delivered at the outcome of the downstream multiplexer. This pulse can be utilized to set the yield of a D flip-flop to '1'. Promote, it is projected to specifically fuse challenge bits into the primitive PUF configuration to bring another layer of arbitrariness for the reaction. Assessment comes about on different devices and under different working temperatures exhibit the applicability of the proposed PUF outline.

- **DAIHYUN LIM, JAE W. LEE, BLAISEGASSEND, G. EDWARD SUH,MARTEN VAN DIJK, AND SRINIVASDEVADAS:**

Modern cryptographic protocols depend on the commence that lone approved members can get secret keys and access to data frameworks or information systems. In any case, different sorts of altering methodologies have been considered to concentrate mystery keys from unforeseen get to frameworks, for instance, smartcards and ATMs. Mediator based physical unclonable limits (PUFs) manhandle the factual defer assortment of wires and transistors across over circuits (ICs) in collecting methodology to manufacture unclonable one of a kind or mystery keys. We made judge based PUFs in custom silicon and investigated the recognizing verification limit, consistency, and security of this arrangement.

Exploratory results and hypothetical audits delineate that a sufficient measure of bury chip exists to engage each IC to be perceived securely and dependably over a down to earth extent of ecological assortments, for instance, temperature and power supply voltage. It exhibit that referee based PUFs are possible and suitable to work, for instance, scratch cards that ought to be impervious to physical assaults.

- **KOTA FRUHASHI, MITSURU SHIOZAKI, AKITAKA FUKUSHIMA, TAKAHIKO.(2011):**

Physical Unclonable Functions (PUFs) is projected as to deliver tamper-resistant device or make exclusive identifications of the protected frameworks or system. The regular essential arbiter-PUF was created with 0.18μm CMOS method, and the uniqueness of produced multi-bit reactions was estimated. The uniqueness is insufficient than anticipated on the grounds that a few of multi-bit reactions are never created. In this review, we recommend a novel arbiter-PUF using a RG-DTM (Response production as indicated by Delay Time Measurement) plot. The uniqueness is assessed by the standard deviation of the Hamming Distance dissemination between created 256-bitresponses. The standard deviation on the proposed PUFs is greatly enhanced to 8.45 from 31 on the traditional PUFs.

- **DOMENIC FORTE AND ANKURSRIVASTAVA. (2013):**

Silicon physically unclonable capacities (PUFs) are circuits that endeavor present day producing varieties to generate unique marks for chip authentication and cryptographic key era. Existing exploration has concentrated on improving PUF quality at structural or configuration levels, yet has unnoticed opportunities accessible amid fabrication, which is the source of systematic and random variation in (ICs)/PUFs. For typical ICs(where security is not a worry), optical proximity correction(OPC) is utilized to smother both these types of variations. Still, a few earlier works have demonstrated that lone systematic variations adversely affect PUF quality and arbitrary variations are helpful for PUFs. In this paper, we propose two PUF-aware OPC cost capacities: 1) P-OPC produces a PUF lithography mask that expands all varieties in PUF circuitry (the inverse of state-of-the-workmanship OPC), and 2) SVC-OPC creates veil patterns that diminish the systematic variation found in PUFs for improved quality. Simulation comes about for ring oscillator (RO) PUFs illustrate that the proposed techniques can enhance PUF signature quality compares to current state-of-the-art OPC.

- **J. W. LEE, DAIHYUN LIM , BLAISEGASSEND, G. EDWARD SUH, MARTEN VAN DIJK, SRINIVASDEVADAS**

This paper portrays a procedure that endeavors the statistical delay varieties of wires and transistors crosswise over ICs to construct a mystery key one of a kind to every IC. To investigate its practicality: we created a hopeful circuit to produce a reaction in light of its postpone qualities. We demonstrate that there exists enough defer variety crosswise over ICs actualizing the proposed circuit to distinguish singular ICs. Promote, the circuit capacities dependably over a commonsense scope of natural variety, for example, temperature and voltage.

- **BLAISEGASSEND, DWAINE CLARKE, MARTEN VAN DIJKY AND SRINIVASDEVADAS(2002)**

Also present the thought of a Physical Random Function(PUF). A complex coordinated circuit can be viewed as a silicon PUF and depict a strategy to identify and verify individual integrated circuits (ICs). We show a few conceivable circuit acknowledge of different PUFs. These circuits have been executed in item Field Programmable Gate Arrays (FPGAs). Wepresent tests which demonstrate that strong confirmation of individual FPGAs can be performed even inside seeing tremendous biological varieties. We depict how secure shrewd cards can be created, and furthermore quickly portray how PUFs can be associated with authorizing and affirmation applications.

- **JAE W. LEE, DAIHYUN LIM, BLAISEGASSEND, G. EDWARD SUH; MARTEN VAN DIJK, AND SRINIVASDEVADAS(2004):**

This paper depicts a strategy that attempts the factual postpone varieties of wires and transistors across over ICs to collect a mystery key uncommon to each IC. To explore its reasonableness: we made a competitor circuit to make a reaction in view of its postpone qualities. We exhibit that there exists enough defer variety crosswise over ICs completing the proposed circuit to perceive particular ICs. The circuit capacities dependably over a handy scope of natural variety, for example, temperature and voltage.

- **MEHRDAD MAJZOOBI AND FARINAZ KOUSHANFAR MIODRAG POTKONJAK**

System security has risen as a head design prerequisite. While there has been a huge group of remarkable work on testing integrated circuits (ICs) desiderata such as manufacturing rightness, delay, and power, there is no reported effort to systematically test IC security in hardware. The objective is to give a force to this line of innovative work by introducing strategies and strategy for thorough testing of physically unclonable functions (PUFs). Lately, PUFs received a incredible arrangement of consideration as security mechanisms because of their flexibility to frame various security protocols and intrinsic resiliency against physical and side channels attacks.

This paper focused on three classes of PUFs characteristic to plan pertinent test method:

(i) predictability,

(ii) sensitivity to component accuracy, and

(iii) susceptibility to reverse engineering.

As our contextual investigations, we examine two prominent PUF structures, linear and feed-forward, and demonstrate that their security is not satisfactory from a few perspectives. The specialized highlights of the paper are the first non-dangerous procedure for PUF reverse engineering and another PUF structure that is able to do passing our security tests.

CHAPTER 3

RESEARCH METHODOLOGY

3.1 IMPLEMENTATION OF ARBITER PHYSICAL UNCLONABLE FUNCTION

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 process varieties prompt one of a kind qualities of these circuits and these unique structure or properties are utilized as signature of the chip. In a multiplexer (MUX) PUF, the delay contrast between the two possible array of a MUX stage is distinctive for each phase in a chip. These varieties are essentially due to design jumble and process variation.

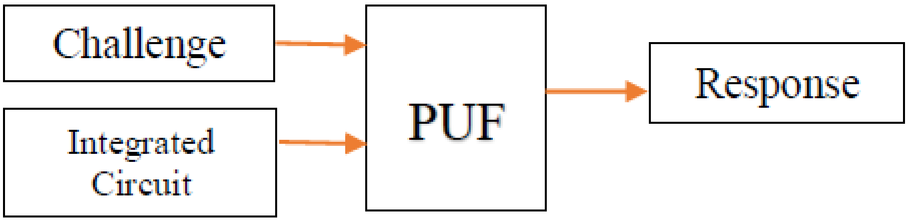

Fig 6: general description of a PUF.

An arbiter PUF is a delay based PUF which is an example of stong silicon PUF. The input to an arbiter PUF is known as a challenge, which is a binary vector whose length is ordinarily same as the quantity of stages in the PUF. The yield is known as a response, which relies upon the delay of their path in the circuit. A randomly picked set of challenge and their corresponding response are called challenge-response pair(CRPs). The PUF's element cannot be detected and its irreproducible attributes to the randomness and the arbitrariness of the manufactering PUF. The delay based PUFs have two preferences which empower to work on-request and to uncover the PUF's trademark through simulation. We concentrate on delay arbiter PUF with respect to which two delay path are simulated at the same time, and the response is chosen by which signal reaches faster.

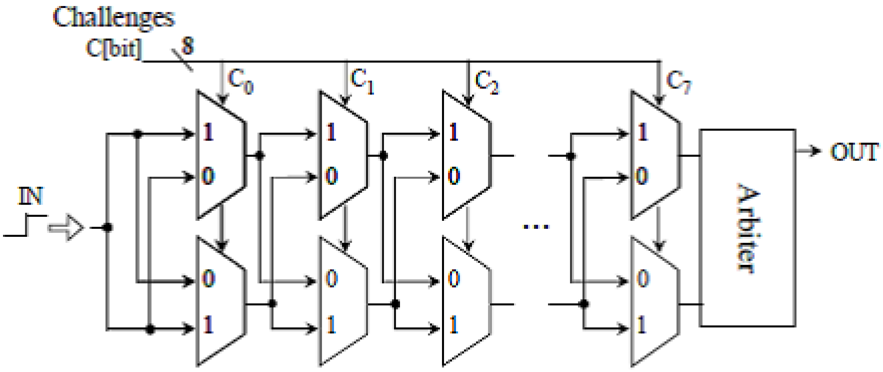

Fig 7: general block diagram of an arbiter delay PUF

As we can see from the block diagram that the input follow two path of the mux PUF and accordingly with the delay introduces by the mux in each path one reaches faster than the other path. And thus we get an either 1 or 0 as the output depending on the path which reaches first. If the upper path reaches first then we get a strong 1 and if the lower path reaches first then we get a strong 0.

3.2 SUB COMPONENTS:

As in the case of many or almost all the electronic devices or circuits, the arbiter mux PUF has its own subcircuits. Among its subcircuits the notable mentions can be described as follows:

3.2.1 MUX

A multiplexer or MUX, which is often called as a data selector, is a combinational circuit with more than one information line or we may say input line, one output line and a distinctive number of select line or switch line depending on the number of the input bit. the function of this device is to choose one of the few analog or digital input signals and forward the chosen data or bit to a single line. A multiplexer of 2n input lines of has select lines of n number which are used to select which of the very input lines have to be selected and send to the output. Multiplexers are predominantly used to expand the measure of information that can be sent over the system inside a specific measure of time and transmission capacity. A multiplexer is thus sometimes also called an input selector or data selector. Multiplexers can likewise be utilized to actualize Boolean elements of various factors. An electronic multiplexer makes it feasible for a few inputs to share one device or resources. An electronic multiplexer can be considered as a multiple input, single-output switch.

Multiplexers, or MUX's, can be either advanced circuits which are produced using fast rationale gates that is utilized to switch computerized or paired information or they can be simple sorts made by utilizing transistors, MOSFET's or relays which are utilized to switch one of the voltage or current contributions through to a solitary yield. For the most part, the choice of each info line in a multiplexer is controlled by an extra arrangement of sources of info called control lines and as per the paired state of these control inputs, either "HIGH" or "LOW" the fitting information info is associated specifically to the yield. Typically, a multiplexer has a much number of 2n information input lines and various "control" inputs that relate with the quantity of information sources of info. Take note of that multiplexers are distinctive in operation to Encoders.

Here as par our convenience for our research work we are using analog type of a 2:1 pass transistor MUX.

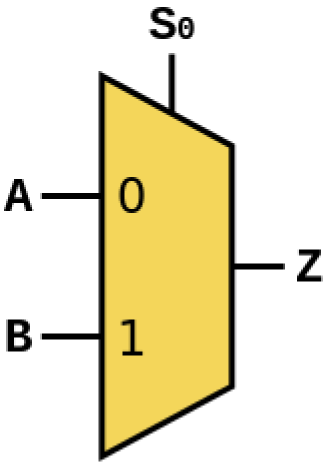

Fig 8: 2:1 mux circuit diagram representation

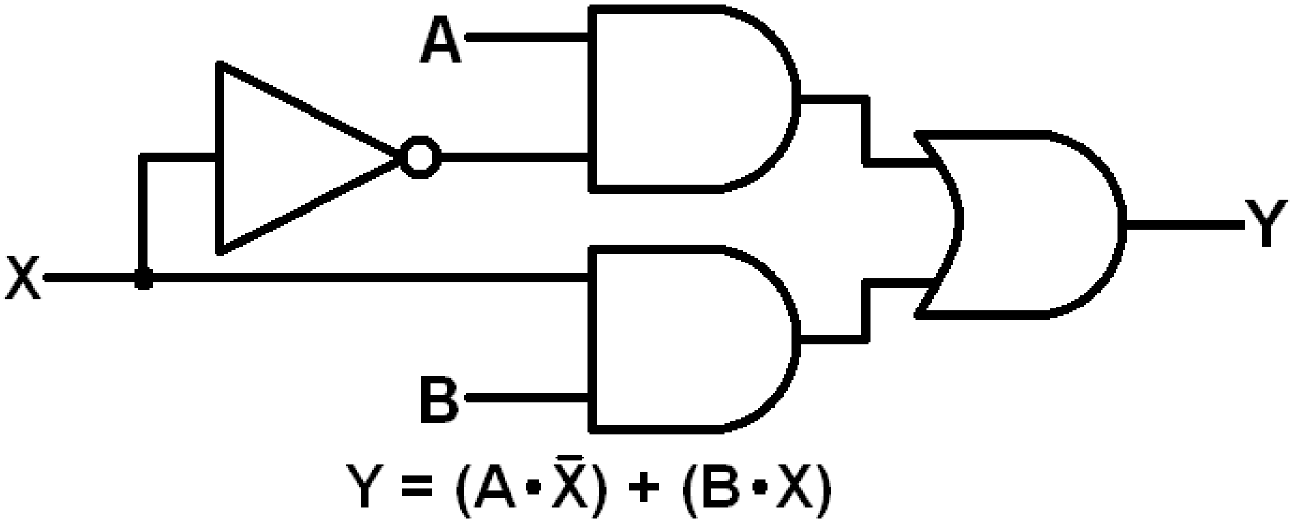

Fig 9: 2-to-1 multiplexer logic diagram using logic gates

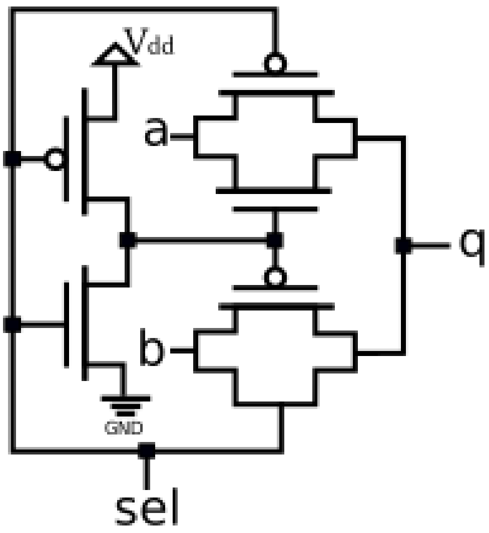

Fig: 2:1 mux using pass transistor

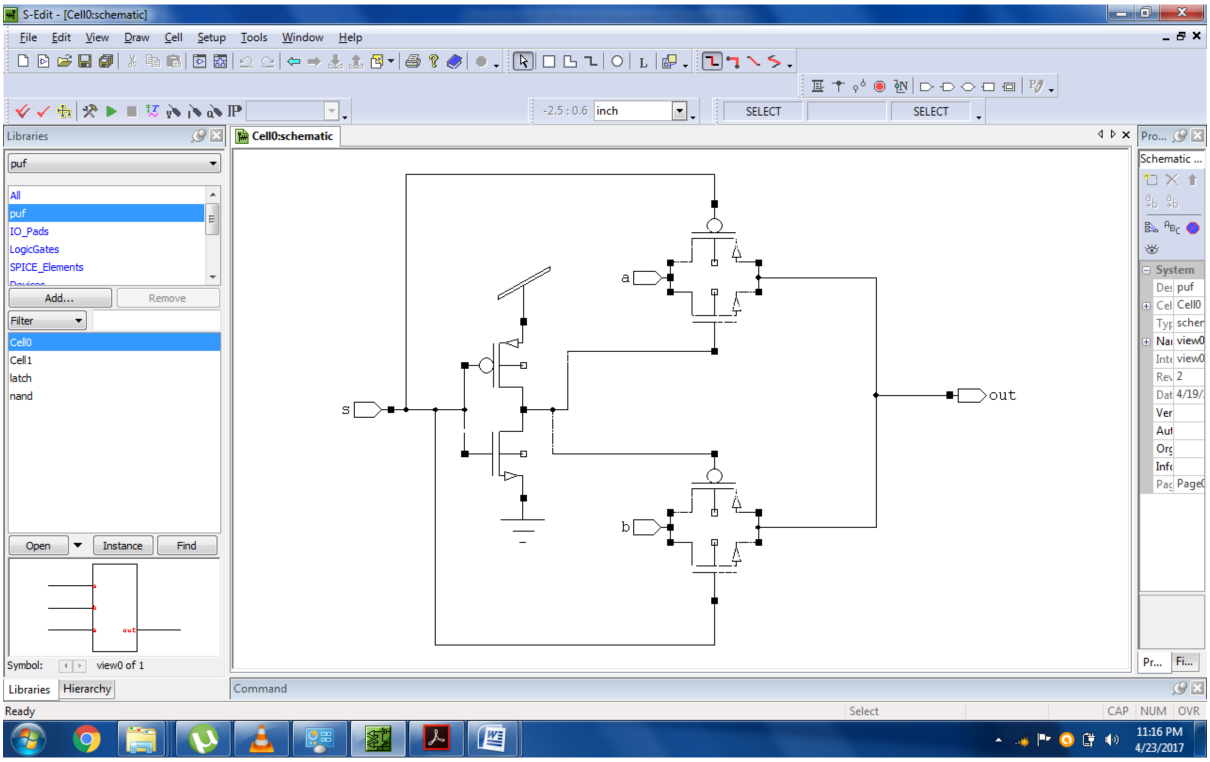

FIG 11: Schematic representation of 2:1 MUX using pass transistor logic

3.2.2 ARBITER CIRCUIT

Arbiter circuit is a special type of circuit designed to respond to the first input reached out of the of two input signals. Here we are using a modified circuit of RS latches.

RS latch are normally constructed by cross-coupled NAND gates made with transistors in connected input and output circuits. As per the innovation, the transistors are estimated and chosen to have relative current limits with the end goal that the estimation of their metastable output voltage is underneath the "trip point" of the following circuit in line so that the metastable voltage is dealt with as a consistent zero value, and accordingly does not propagate through the system.

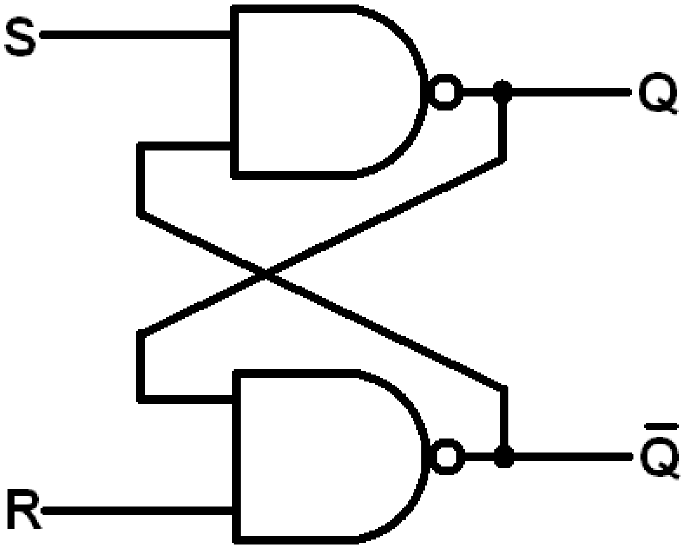

Fig 12: A simple SR latch

It is notable that such circuits experience the adverse effects of an inherent issue, specifically that, if two data sources begin to rise at the same time, or if there is a noise pulse on either of the input, the circuit may switch state just partly. This condition is called a metastable state as it lasts for an undefined time which is comparatively long as to the switching time of the circuit, but is shorter than that of a conventional pulse width time. this might cause a circuit which is connected next in line to response to a metastable state and might produce an unwanted signal which probably will propagate further to produce unexpected responds or output.a It is also possible for the output of the latch to oscillate, producing a train of pulses.

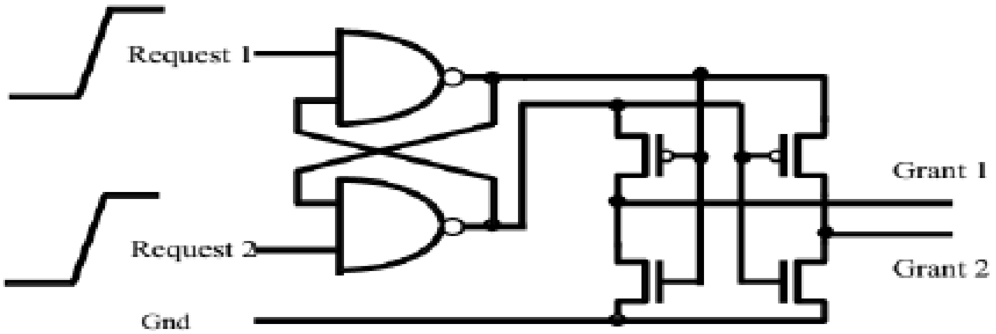

Fig 13: Metastable state arbiter

The figure above represents an arbiter circuit in which the input are each connected through a NAND gate to an inverter, which acts as a discriminator, and them to corresponding respective output terminals. The two NAND form a conventional RS latch. It is known fact that, if the voltages on both inputs rises at the same time, or within the settling time of the circuit, the circumstance will be unstable, in which both NAND gates will be battling to set up control, i.e. which one's input will control the output signals. This "metastable" state will flip in a short however vague timeframe to one of the two stable voltage states or back to the quisient state. In any case, when two inverters acting as discriminators, are connected respectively to their outputs of the regular RS latch,the metastable voltage alone won't be dependably either above or underneath the trip point of inverters, so it is unrealistic to foresee, ahead of time, what the output voltages of the inverters will be when there is a metastable state display.

As per the new innovation, the present limits of the transistors utilized with NAND gates are changed so that there is an anticipated metastable voltage present on the output terminals, and this voltage is set to be dependable on one side or the other of the trip point of the discriminator.

3.3 SIMULATION OF ARBITER PUF

In this paper, we are doing simulation method to test and analyse the power and reliability of the PUF rather than fabrication method. Here we are implementing a simple linear PUF of 28 stages in 180nm technology, a feed- forward PUF of 14 stages in 65 nm and a feed-forward PUF of 14 stages using double gate MOSFET in 45nm. We are using Tanner EDA tool which includes s-edit, t-spice, w-edit. The feed-forward PUF of 14 stages is the model proposed here in this research work.

3.3.1 POWER AND RELIABILITY MEASUREMENT OF BASIC MUX AND STANDARD FEED FORWARD

- **Performance Analysis of Basic MUX PUF**

Here, we have taken 28-stage basic MUX PUF in 180nm technology. 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 the select line in the order of 0 1 1 1. The model is simulated at 0°C, 27°C, and 100°C.

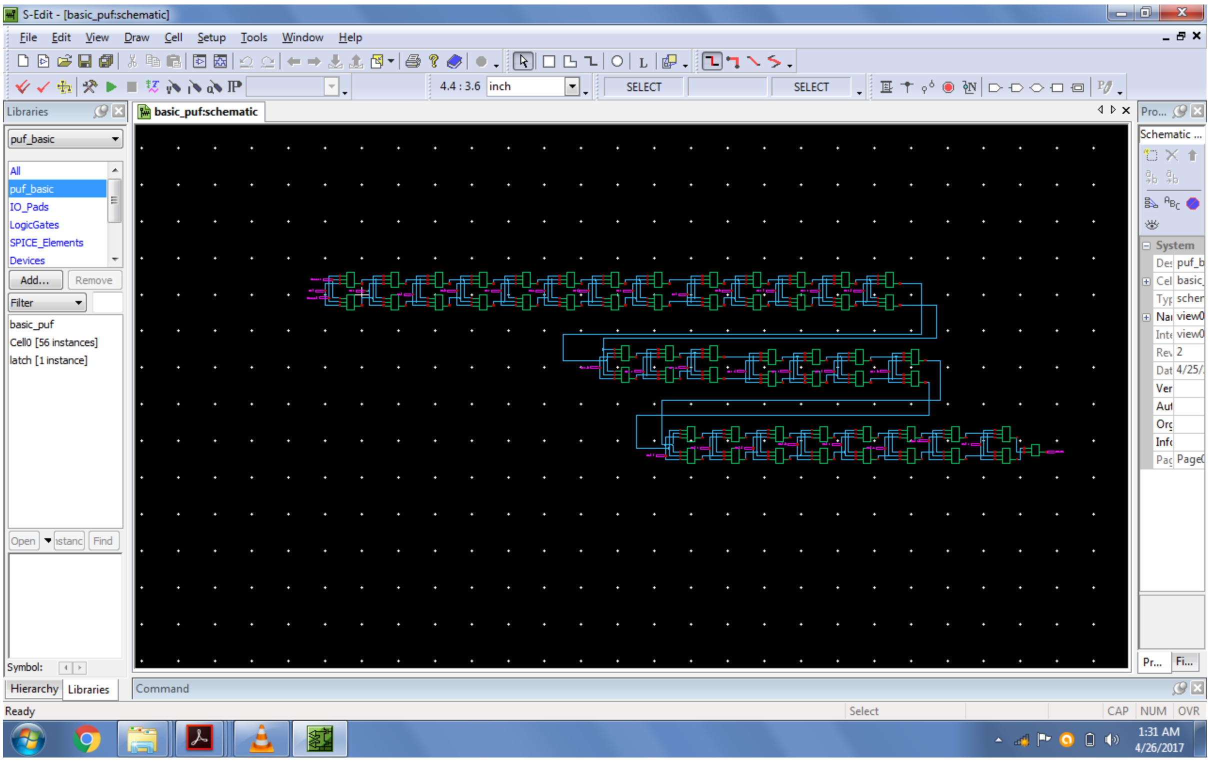

Fig 14: Schematic diagram of basic mux PUF

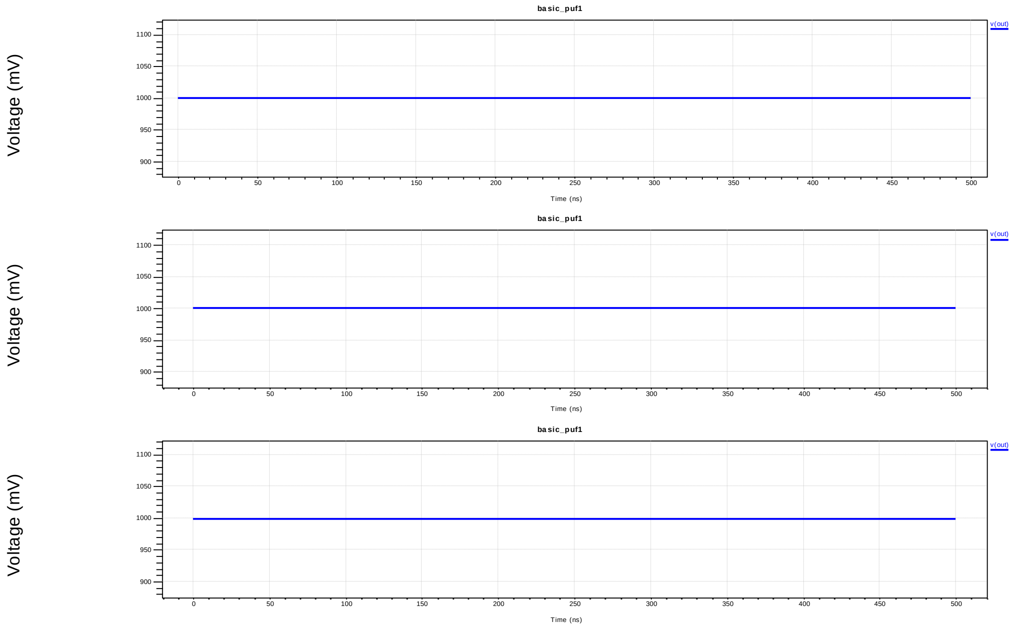

Fig 15: Analog simulation output performed at 0°C, 27°C AND 100°C

The intra chip variation thus obtained from the simulation is 0. So the reliability for the basic MUX PUF is concluded to be 100%. But since this kind of PUF gets easily attack, even though it has the highest reliability among all the PUF model it is not used for application based hardware.

- **Performance Analysis of feed-forward MUX PUF**

Here, we have taken 14-stage feed-forward MUX PUF in 65nm technology. 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 the select line in the order of 0 1 1 1. The output is simulated at 0°C, 10°C, 25°C and 35°C.

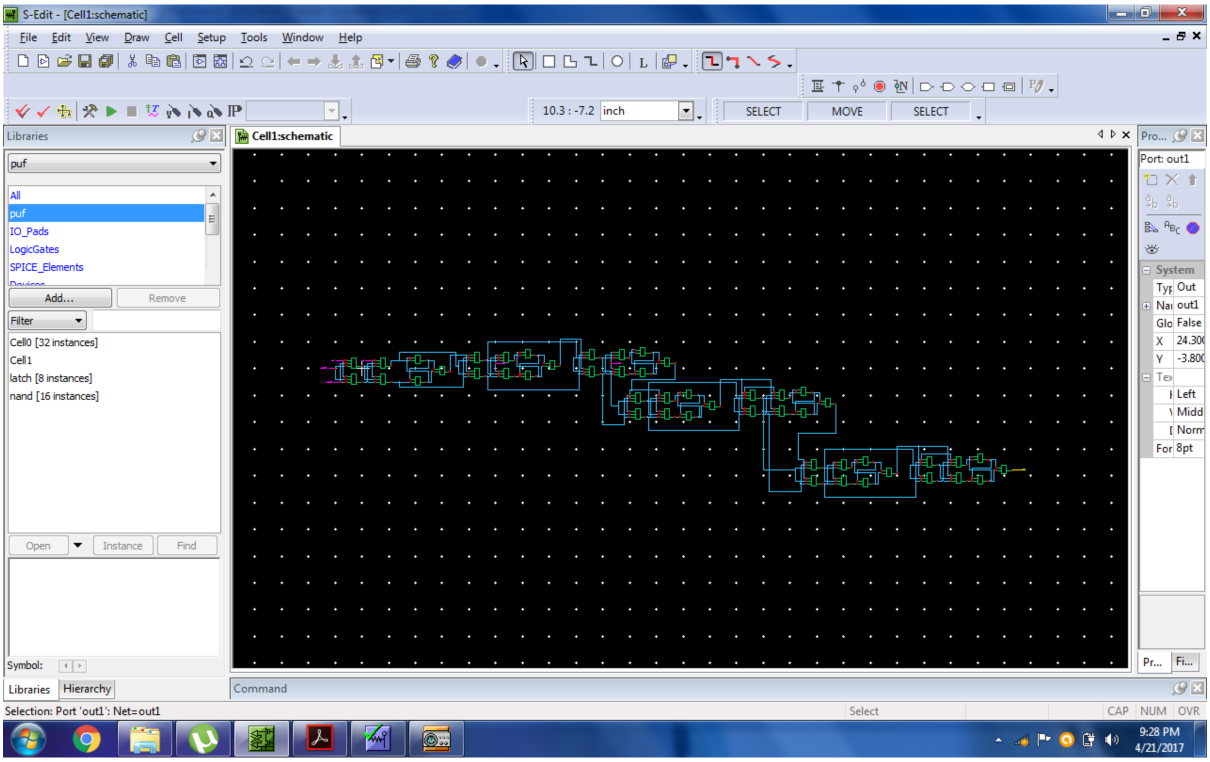

Fig 16: Schematic diagram of 14 stage feed-forward MUX PUF

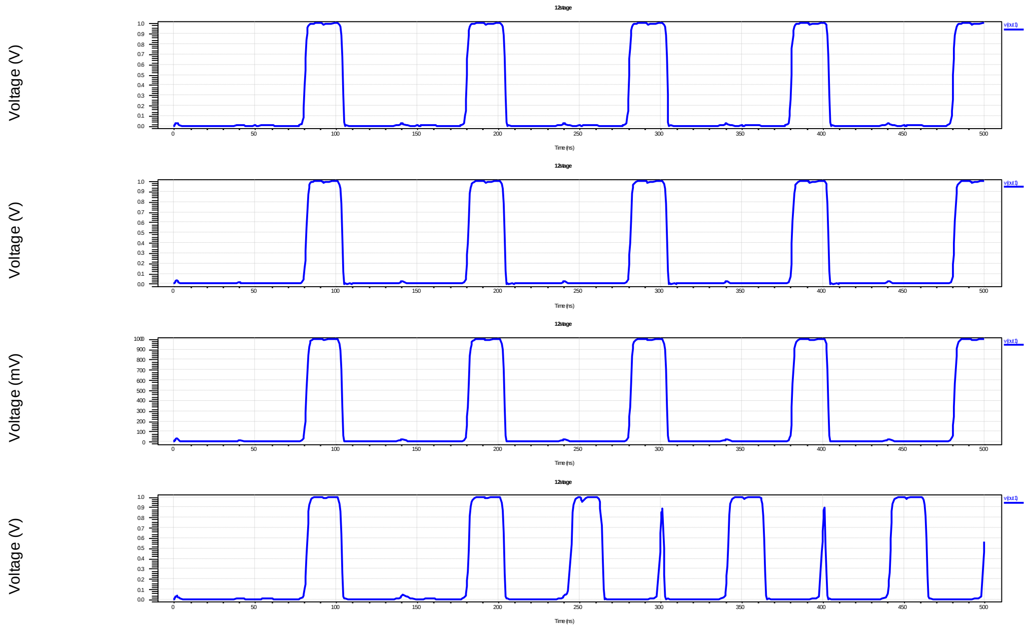

Fig 17: Analog simulation output performed at 0°C, 10°C, 25°C and 35°C.

The intra chip variation thus obtained from the simulation is 1.2. So the reliability for the basic MUX PUF is concluded to be 98.8. It can be seen from the output waveform that the output variations starts at about 35°c. so this puf is applicable within the temperature range of 0 to 35°c. The average power obtained through the simulation is 52.3uW.

3.3.2 THE PROPOSED MODIFIED FEED FORWARD MUX PUF

Here we have implemented the PUF using double gate MOSFET of 45nm technology. DGT is comprised of a drain, source, and two gates with conducting channel surrounded by gate electrodes on either side. This guarantees no a portion of the channel is far from a gate node.

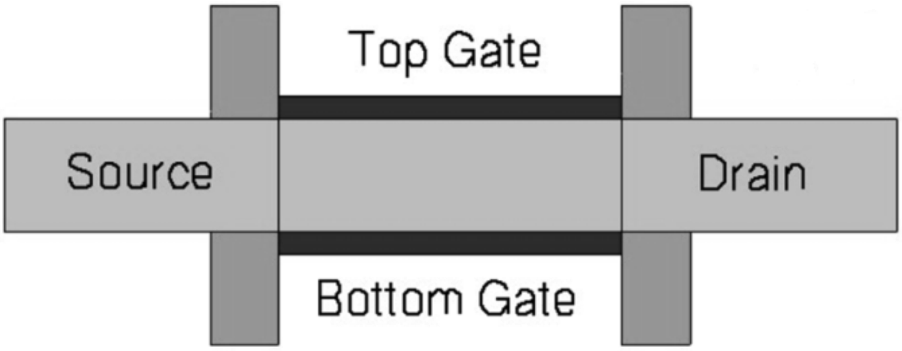

Fig 18. Device Structure of Double Gate MOSFET

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.

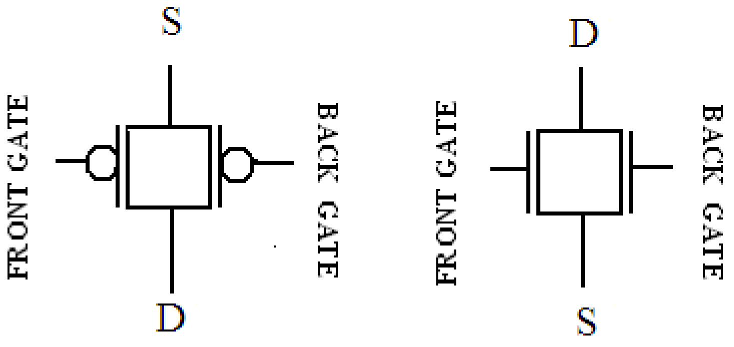

Fig 19. Circuit symbols for DG-PMOS and DG-NMOS

Here we are showing the implementation of feed forward PUF and its sub components using double gate MOSFET.

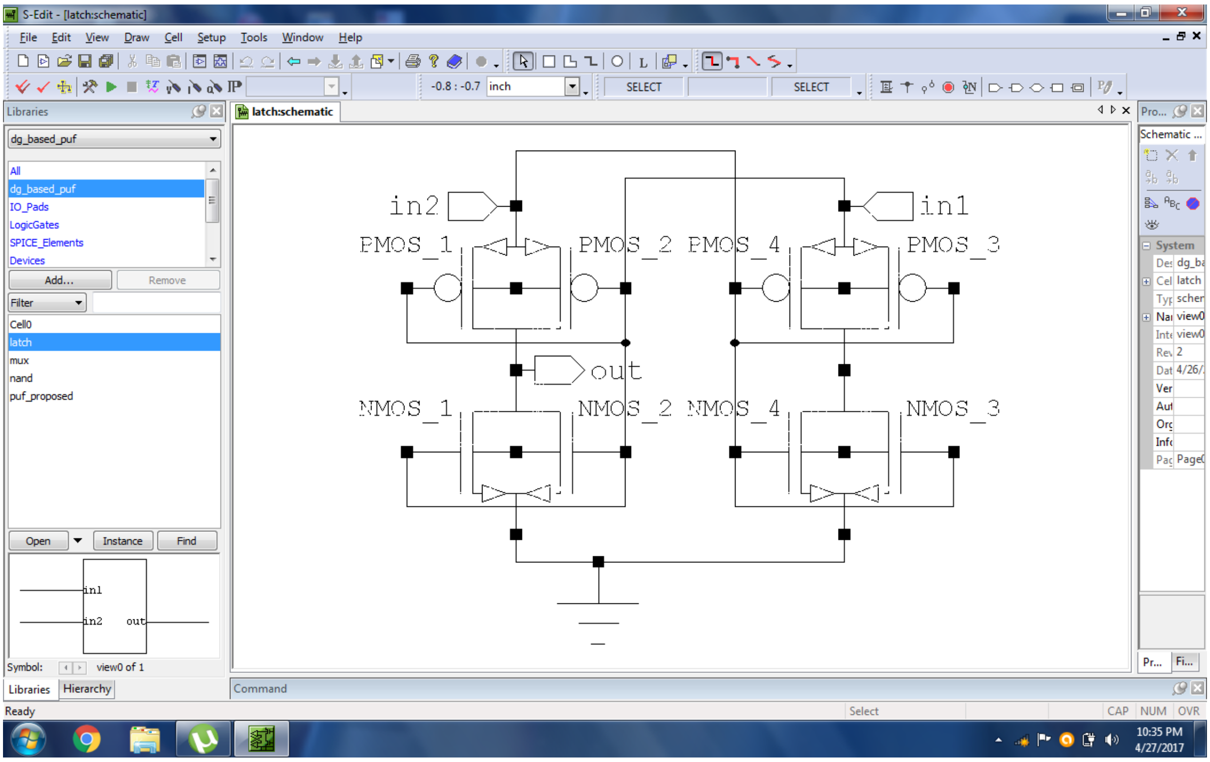

Fig 20: Schematic of arbiter circuit using DG MOSFET

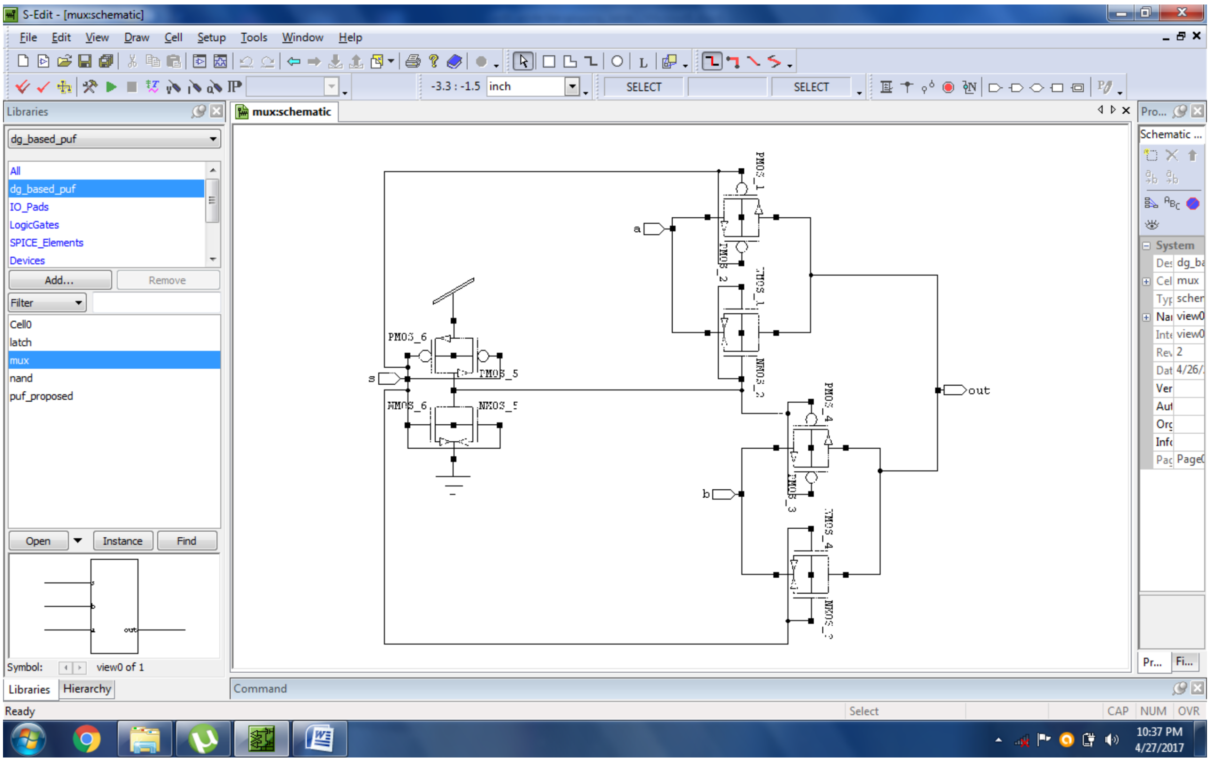

Fig 21: Schematic representation of 2:1 mux using DG MOSFET

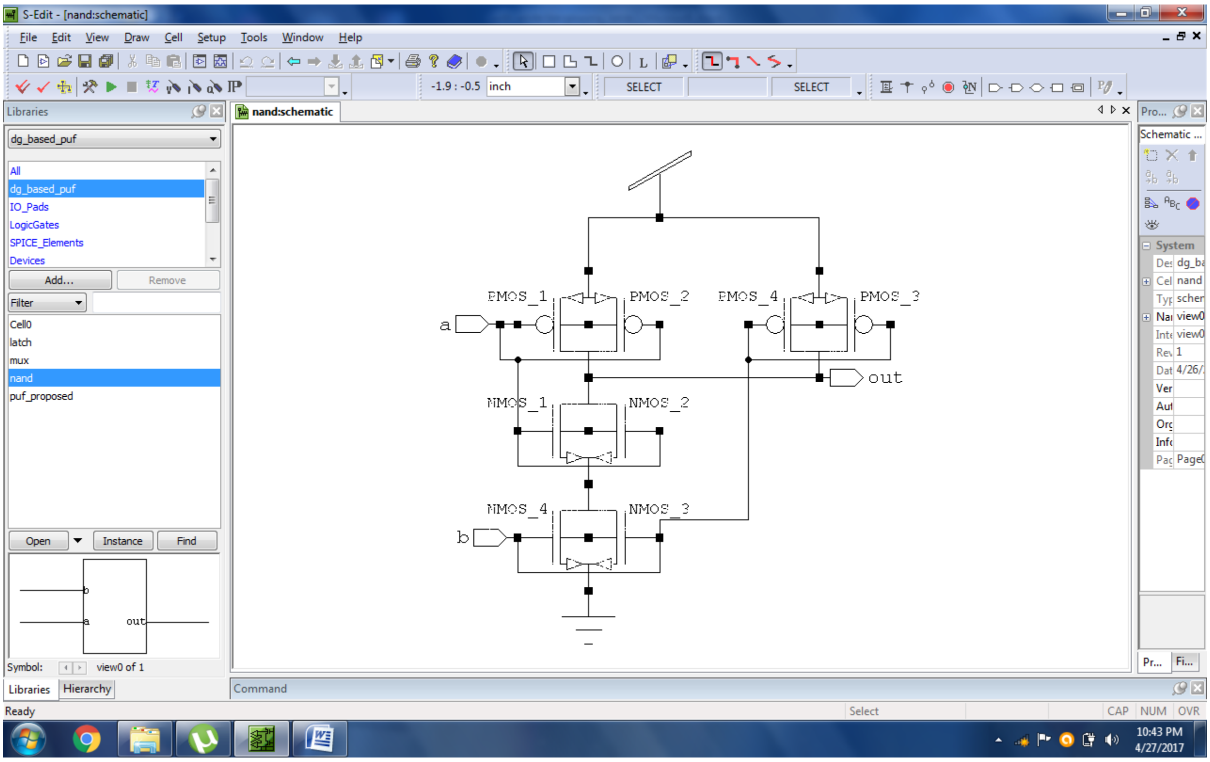

Fig 22: Schematic representation of NAND gate using DG MOSFET

- **Power and reliability analysis of proposed feed-forward MUX PUF**

Here, we have taken 14-stage feed-forward MUX PUF in 45nm technology. 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 the select line in the order of 1 0 0 1. The output is simulated at -5°C, 0°C ,10°C and 25°C.

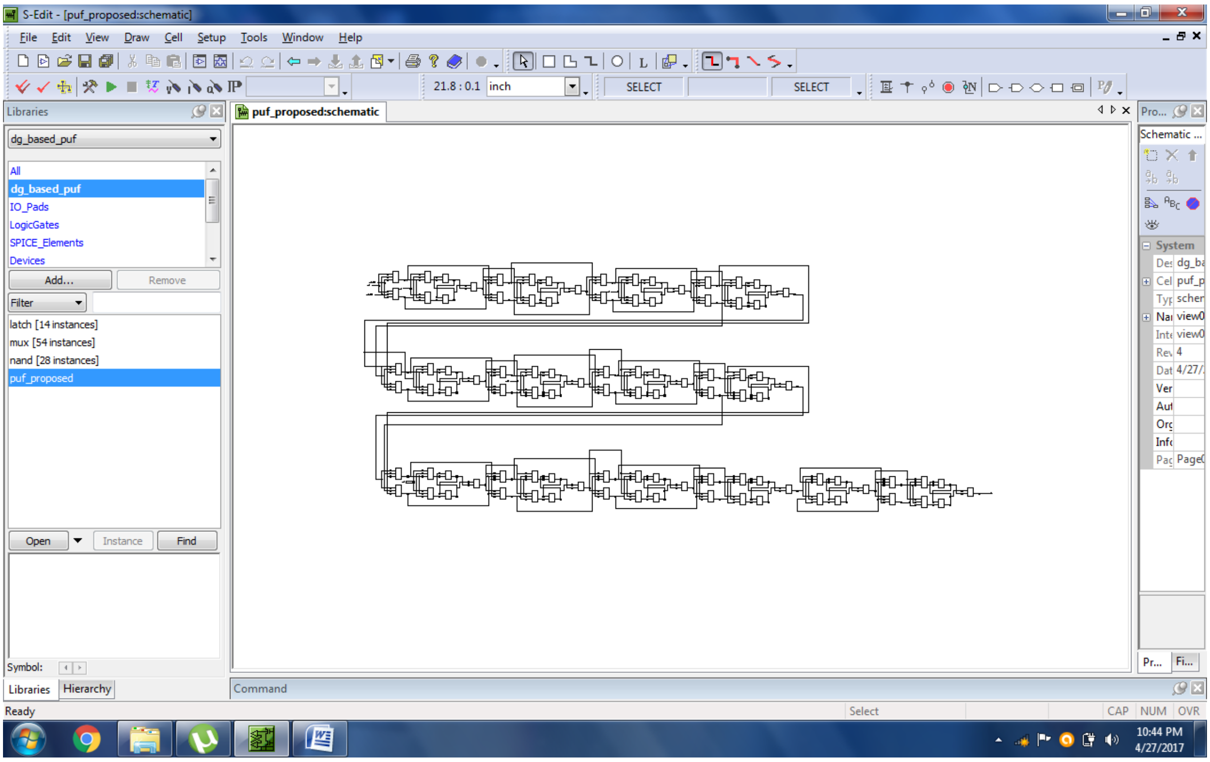

Fig 23: Schematic diagram of 14 stage feed forward PUF using DG MOSFET

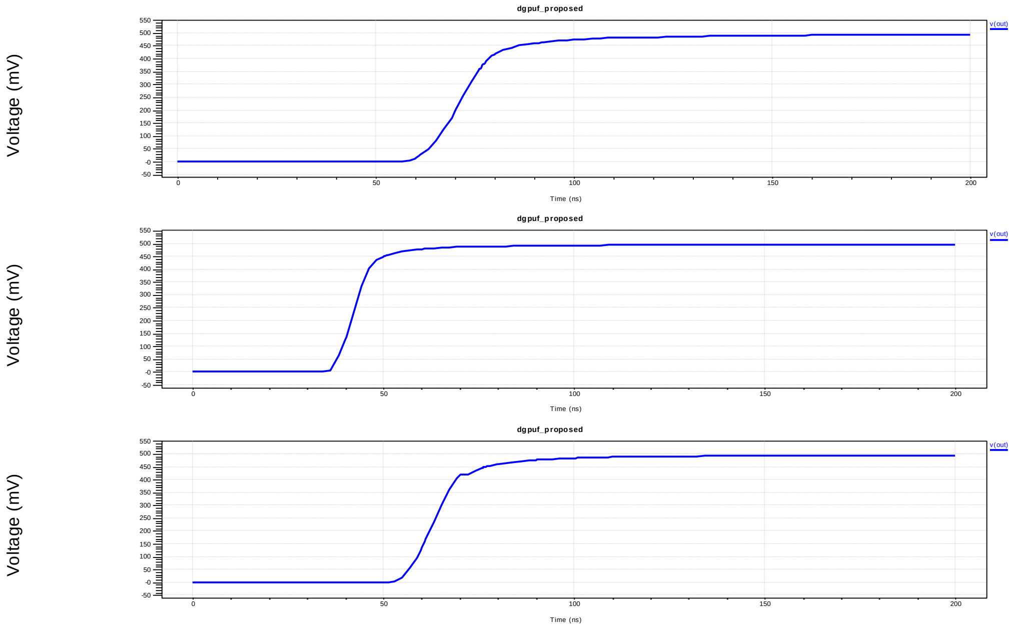

Fig 24: Analog simulation output performed at -5°C, 0°C and 10°C

The intra chip variation obtained from the simulation is 0.78%. So the reliability for the proposed MUX PUF is concluded to be 99.22% . It can be seen that the output variations starts at about 25°c. so this puf is applicable within the temperature range of -5°C to somewhere below 25°C. The average power obtained through the simulation is 2.5 uW.

CHAPTER 4

PERFORMANCE COMPARISION OF THE VARIOUS MUX-BASED PUF

4.1 SIMPLE LINEAR MUX-PUF

Parameters	Data
V_{dd}	1.8
technology	180nm
stage	28
power	80nw
reliability	99.9%
security	Less

4.2 COMPARISION OF SIMPLE FEED-FORWARD MUX PUF AND FEED-FORWARD MUX PUF USING DG MTCMOS

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)	50uw	2.5 uw

CHAPTER 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. 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 modelling technique.

CHAPTER 6

REFERENCE

1. Pappu, R.; Recht, B.; Taylor, J.; Gershenfeld, N. "Physical One-Way functions". Science 297 (5589): 2026–2030. doi:10.1126/science.1074376.
2. Md. Tauhidur Rahman, Student Member, Fahim Rahman, Student Member, Domenic Forte, Member, and Mark Tehranipoor," An Aging-Resistant RO-PUF for Reliable Key Generation" 2014
3. S. V. Sandeep Avvaru, Chen Zhou, Saroj Satapathy, Yingjie Lao, Chris H. Kim, Keshab K. Parhi "Estimating Delay Differences of Arbiter PUFs sing Silicon Data" Department of Electrical and Computer Engineering University of Minnesota Minneapolis, MN 55455 USA
4. B. Gassend, D. Clarke, M. van Dijk, and S. Devadas, "Silicon physical random function s," in Proceedings of the 9th ACM Conference on Computer and Communications Security, 2002, pp. 148- 160.
5. J. Lee, D. Lim, B. Gassend, G. Suh, M. van Dijk, and S. Devadas, "A technique to build a secret key in integrated circuits for identification and authentication application s," in Symposium on VLSI Circuits Digest of Technical P apers, June 2004, pp. 176-179.
6. M. Majzoobi , F. Koushanfar, and M. Potkonjak, 'Testing techniquesfor hardware security; ' in Proceedings of IEEE International Test COf!{erence (ITC) , Oct 2008, pp. 1- 10.
7. Yingjie Lao, Student Member, Keshab K. Parhi, Fellow"Statistical Analysis of MUX-Based Physical Unclonable Functions" ieee transactions on computer-aided design of integrated circuits and systems, vol. 33, no. 5, may 2014.
8. "https://en.wikipedia.org/w/index.php?title=Physical_unclonable_function&oldid=714205859"
9. "https://en.wikipedia.org/w/index.php?title=Types_of_Physical_unclonable_function&oldid=692512812"
10. Rahim Pegu, Rajkishur Mudoi "Design and Analysis of Mux-based Physical Unclonable Functions" International Journal of Engineering Research & Technology (IJERT) ISSN: 2278-0181 Vol. 4 Issue 05, May-2015.

11. 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.
12. H. Chang and S. Sapatnekar, “Statistical timing analysis considering spatial correlation in a pert-like traversal,” in IEEE International Conference Computer-Aided Design Integrated Circuits and Systems, 2003, pp. 621–625.
13. 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 and authentication applications,” in IEEE International Conference Computer-Aided Design Integrated Circuits and Systems, 2003, pp. 621–625.
14. K. Kursawe, A. Sadeghi, D. S. B. Skoric, and P. Tuyls, “Reconfigurable physical unclonable functions – enabling technology for tamper-resistant storage,” in 2nd IEEE International Workshop on Hardware-Oriented Security and Trust(HOST), 2009, pp. 22–29.
15. Daihyun Lim, Jae W. Lee, Blaise Gassend, G. Edward Suh, Marten Van Dijk, and Srinivas Devadas “Extracting secret keys from integrated circuits” ieee transactions on very large scale integration (vlsi) systems, vol. 13, no. 10, october 2005

APPENDIX

AUTOBIOGRAPHY

I, KONSAM JEMSON MEITEI is currently pursuing M.Tech in Electronics and Communication Engineering from Lovely Professional University, Phagwara with VLSI as my specialization.

dessertation.docx

ORIGINALITY REPORT

%18	%4	%15	%3
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	Yingjie Lao, , and Keshab K. Parhi. "Statistical Analysis of MUX-Based Physical Unclonable Functions", IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, 2014. Publication	%2
2	Mustapa, Muslim, and Mohammed Niamat. "Novel RPM technique to dismiss systematic variation for RO PUF on FPGA", NAECON 2014 - IEEE National Aerospace and Electronics Conference, 2014. Publication	%2
3	Forte, Domenic, and Ankur Srivastava. "Improving the Quality of Delay-Based PUFs	%1