“DESIGN OF PHYSICAL UNCLONABLE FUNCTIONS WITH DELAY FOR HARDWARE SECURITY”

DISSERTATION-II

Submitted in partial fulfillment of the

Requirement for the award of the degree

Of

MASTER OF TECHNOLOGY
Electronics & Communication Engineering
By

MEGHANA SAGAR

(11308728)

Under the Esteemed Guidance

Of

Mr. Jyotirmoy Pathak

Assistant Professor (LPU)

School of Electronics & Electrical Engineering
Lovely Professional University
Punjab
NOV 2017

INDIA'S LARGEST UNIVERSITY

LOVELY PROFESSIONAL UNIVERSITY

Transforming Education, Transforming India

TOPIC APPROVAL PERFORMA

School of Electronics and Electrical Engineering

Program : 1205D::B.Tech -M.Tech (Dual Degree) - ECE

COURSE CODE : ECE620 **REGULAR/BACKLOG :** Regular **GROUP NUMBER :** EEERGD0061

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

Qualification : ________________________ **Research Experience :** ________________________

SR.NO.	NAME OF STUDENT	REGISTRATION NO	BATCH	SECTION	CONTACT NUMBER
1	Kallepu Meghana Sagar	11308728	2013	E1321	9465323738

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

PROPOSED TOPIC : Design of Physical unclonable Function with delay 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	7.00
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.	7.00
4	Project Supervision: Project supervisor's is technically competent to guide students, resolve any issues, and impart necessary skills.	7.50
5	Social Applicability: Project work intends to solve a practical problem.	7.50
6	Future Scope: Project has potential to become basis of future research work, publication or patent.	7.50

PAC Committee Members		
PAC Member 1 Name: Anshul Mahajan	UID: 11495	Recommended (Y/N): Yes
PAC Member 2 Name: Cherry Bhargava	UID: 12047	Recommended (Y/N): Yes
PAC Member 3 Name: Dushyant Kumar Singh	UID: 13367	Recommended (Y/N): NA
DAA Nominee Name: Ishan Luthra	UID: 15330	Recommended (Y/N): NA

Final Topic Approved by PAC: **Design of Physical unclonable Function with delay for hardware Security.**

Overall Remarks: Approved

PAC CHAIRPERSON Name: 11211::Prof. Bhupinder Verma **Approval Date:** 31 Oct 2017

11/30/2017 2:09:31 PM

CERTIFICATE

This is to certify that the Dissertation-II titled “**Design of Physical Unclonable Functions with delay for hardware security**”. That is being submitted by “**Meghana sagar**” in partial fulfillment of the requirements for the award of Master of Technology, 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 forward of any degree or diploma and the same is certified.

Mr. Jyotirmoy Pathak
`
Supervisor
Assistant Professor
(Lovely Professional University)

Objective of the Thesis is satisfactory/unsatisfactory

Examiner I **Examiner II**

ABSTRACT

Physically Unclonable Functions (PUFs) have turned a new page in hardware security by presenting a promising technique in security. PUFs are based on challenge-response scheme, where instead of calculating the response they are determined by the randomness due to manufacturing variabilities in devices. Behavior of each PUF is different even when manufactured under same external conditions. An arbiter PUF utilizes the race condition between equally designed delay paths. This thesis deals with enhancement and stimulation of arbiter PUF. PUF is broadly categorized into two namely weak PUF and strong PUF. Weak PUFs are mostly used for secret key generation and authentication is done by strong PUFs. Various linear and nonlinear PUFs like FF, FFO, FFS, FFC et.al. are key parts in this thesis. Finally, implementation of 16 bit and 25 bit PUF if done and presented along with description about basic architecture and components of PUF. Response from the implemented PUFs is analyzed by performance parameters namely reliability, uniqueness and randomness.

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 who 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 guided me to take up this thesis in sync with global trends in scientific approach.

I owe my heartiest thanks to my parents & all those guideposts who really acted as lightening pillars to enlighten my way throughout this project that has led to successful and satisfactory completion of my Dissertation-II.

Last but not least, I would like to thank God for the strength that keeps me standing and for the hope that keeps me believing that this report would be possible. I would also thank the staff members of the department of Electronics and Communication engineering who have been very patient and co-operative with us.

DECLARATION

I, Meghana Sagar, student of Master of Technology under Department of Electronics and Communication 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 work which is not done by me.

Date:

Meghana sagar

Reg.No. 11308728

M.Tech (ECE)

Lovely Professional University

LIST OF CONTENTS:

S.NO **NAME OF CHAPTER** **PAGE.NO**

LIST OF FIGURES

LIST OF ABBREVATIONS:

PUF	Physical unclonable functions
MUX	Multiplexer
DEMUX	De multiplexer
FF	Feed forward
FFO	Feed forward overlap
FFC	Feed forward cascade
FFS	Feed forward separate

CHAPTER 1

INTRODUCTION:

As we see, in our modern-day world embedded devices and mobiles are becoming interconnected platforms. These interconnected platforms are part of almost everyday tasks. internet of things, home automation, intelligent air-conditions, washing machines, refrigerators have already become a part our life. the major part of these tasks is to securely handle our private information and a secure authentication must both sides. The days where people use to go for bank to perform bank transactions are long gone. nowadays everything can be done sitting in our chair including every account details and bank transactions. Smartphones have become a unified platform which are now capable of conducting the most secure financial transactions, able to securely store the information of user, acting as a token of authentication for the user and conducting many more operations securely [1].

As a powerful hardware for mobile computing is developed, it has provided a flexibility in software to enable convenient processing of mobile data. However, compared to software security, development in hardware security has been slower. Our hardware can be in different environments sometimes it may fall into the hands of an adversary. When there is a physical access to the system, the degree of losing our data to an adversary is high.

The present day best followed practice to secure such hardware's is storing the secret key in nonvolatile memory sources and securing the memory sources. The secret key is a key which prevents the adversary from attacking our hardware and helps us access our hardware. The nonvolatile memory can be SRAM (static random access memory) or EPROM (electrically erasable programmable read only memory). Also hardware security operations like cryptography using digital signature or encryption is used.

We know that the important parameters in designing the hardware are cost, area and power consumption. The above mentioned methods are very expensive, increasing the area of design and also increasing the power consumption. As mentioned above secret keys are stored in nonvolatile memory sources. These nonvolatile memory sources are very much vulnerable to many attacks such as invasive attack mechanism. To prevent these attacks, we must provide a constant active tamper prevention mechanism or provide constant detection mechanism. This process increases the circuitry. This circuit must be constantly powered and it increases power consumption. The above mentioned method also increases the overall time delay of the circuit.

Physically unclonable functions (PUFs) are primitive innovative promising circuits that are used to serve their main purpose of authentication and are also used to generate the secret key along with the capability to store them and does not require the above mentioned expensive, power consumed large circuitry. We are able to this because instead of storing the secret key in the nonvolatile memory, PUF generates a secret key depending upon on the physical parameters of the integrated circuits. There are few parameters in the integrated circuits which cannot be controlled during manufacturing of circuits. PUF realizes these uncontrollable parameters due to manufacturing variations and converts them into a readable form. The realized uncontrollable parameters of PUF can be used as a secret key. This secret key can know be used for authentication or cryptographic techniques depending upon our application.

These uncontrollable physical parameters can be of many types like delay, leakage currents, trapped capacitances, metastability in memory devices etc. In this paper we concentrating on one of the physical parameter delay because delay is the most primary uncontrollable parameter caused in almost all the circuits due to variations at the time of manufacturing. Also delay is comparatively easy to realize than the other physical parameters.

The below mentioned are the few advantages of PUF above other standard protocol:

- Instead of using expensive anti tamper memory sources (SRAM/EPROM), the circuitry of PUF hardware is simple digital circuit which is easy to manufacture, requires less area and consumption of power is less. Also, we can replace the application of PUF with expansive cryptographic hardware techniques which uses secure hash algorithm (SHA) and also replaces encryption algorithms which uses public and private keys.
- As we discussed, in PUF we derive our secret key from the physical parameters of integrated circuit. therefore, extraction of any information regarding the secret key must be done when the device is powered on. so, any physical attack can be done on the only when the chip is powered up.
- Invasive attacks on PUF are more difficult, because to extract the secret key from PUF, its physical parameters must not be altered. This makes execution of invasive attacks more difficult on PUF. As the invasive attacks are almost not possible we do not need expensive, power consuming anti tamper mechanisms for security of PUF.
- Manufacturing of nonvolatile memories is a lot expensive process. Additional mask layers are required for EPROMs and RAMs always require external power sources. in case of PUF these are not required.

The basic concept of PUF is that even though if different integrated circuits are manufactured with manufacturing process, the uncontrollable parameters differ from one circuit to other due to their manufacturing variabilities. This leverage of

PUF makes it special. The secret key derived from each PUF can act as a biometric for the particular integrated circuit. Also, even if the attacker knows the complete manufacturing process of a PUF, it impossible to clone the exact PUF due its manufacturing variabilities. So, this feature of PUF makes it special from other encrypting algorithms. Its uniqueness helps us to authenticate the chip creating a unique biometric which does not match with any other key even the full knowledge of manufacturing process.

CHAPTER 2

LITERATURE REVIEW:

S.V. SANDEEP AVVARU et.al [3]: In this paper they have presented a novel approach in estimating the differences of delay in each stage of standard MUX based PUF. They have used two different models to map the relation between challenge and response pairs. The two algorithms used are LMS (least mean square algorithm) and perceptron algorithm. With the help of these two models they estimated the delay differences between each MUX. With least mean square algorithm they achieved the accuracy from 97.5% to 99.5% and with perceptron algorithm they have achieved accuracy of 100%. Comparison between the results of least mean square algorithm and perception models is done. A scaling factor is computed from the comparisons. From the analysis of the above models it was concluded that the delay differences of different stages in MUX PUF belong to the same Gaussian probability density function.

S.V. SANDEEP AVVARU et.al [4]: In this paper a novel concept of hard and soft responses of PUF is proposed. The probability of the response bit to be ‘1’ is referred as soft response and the probability of the response bit to be ‘0’ is referred to as hard response. In this paper an artificial neural network has been proposed to predict hard and soft responses. evaluation of standard arbiter PUF, feed forward PUF and modified feed forward PUF using the proposed model is done. At first, the unpredictability of PUFs is evaluated by using hard responses. These hard responses are predicted using the proposed artificial neural network model. The probability obtained is compared with the original results of PUF. Secondly, the proposed artificial neural networks are trained to predict the soft responses. Stability is defined by the threshold scheme based on probability.

Finally, the obtained hard and soft responses are used to predict the challenge response pairs.

BLAISE GASSEND et.al [5]: In this paper, the notion of physical random functions is introduced which argue about the PUF technique. Initially the basic definition of PUF is given then an overview of manufacturing variations and environmental variations are given. The basic description of challenge response pairs is given. Then it is described that how a PUF can be attacked and different possible ways of attacking a PUF. followed by architecture and implementation of PUF. A basic overview of how PUF provides the security is given. Brief description about linear and nonlinear delay models of PUF. Then error control mechanism of PUF is described. Then how authentication is done by PUF. Followed by how to prevent attacks on PUF. Finally, various applications of PUF are mentioned.

YINGJIE LAO et.al [2]: In this paper initially a brief description about delay based MUX PUF is given. Implementation of both linear and non-linear PUF is done. A brief description of different kinds of delay based nonlinear feed forward MUX PUF is given. They are feed-forward overlap MUX PUF (FFO), feed forward cascade MUX PUF (FFC), feed forward separate MUX PUF (FFS) and MUX/DEMUX PUF. Three important parameters for the performance evaluation of delay based MUX PUF are given along with them mathematical modelling, they are namely reliability, uniqueness and randomness. These performance parameters are calculated based on intra and interchip variables. a brief description about MUX based reconfigurable PUFs is given. The reconfigurable PUFs are of two types they are CRP-reconfigurable PUF and logical reconfigurable PUF. Initially standard MUX based PUF was implemented different stages with N=25,50,75,100,125,150. Considering the three performance parameters, they concluded that at N=100 the results are better and with N=100, they implemented the above mentioned FFC, FFO, FFS and MUX/DEMUX PUFs. They even provided a modified version of FFC, FFO, FFS and MUX/DEMUX PUFs and are also implemented at N=100. Finally, a comparison of results between the normal and modified version is done with the help of performance parameters.

YANGJIE LAO et.al [6]: In this paper a more secure and reliable PUF authentication is proposed with an extra feature of lightweight. A finite state machine (FSM) in two levels is proposed to correct erroneous bits generated by environmental parameters. The environmental parameters can be temperature, aging and voltage. This method eliminates the problem of counterfeiting. By using this two level FSM the rea consumed will be reduced to by 2 to 10 times and the power consumption reduces by 20 to 100 times when compared to BCH codes. According to the experimental results in this paper the cost of the above mentioned two level self-correcting FSM is reduced significantly when compared with codes of error correcting. The performance and applications of the two level self-correcting FSM are also discussed. In this method they mapped each and every PUF response with a key and the actual is generated only after the fabrication of the integrated. This way the adversary is not known about the key and counterfeiting effect is prevented. Each state of FSM is determined with each response of the PUF.

MEHRDAD MAJZOOBI et.al [7]: In this paper xor gates are used to increase the randomness of the response generated by the PUF. Three main working features in this PUF are each response bit is created by including multiple delay lines, challenge bits are not directly provided to each MUX stage, they are combined and transformed before they reach MUX stage and the outputs obtained from multiple delay lines are combined to make final response. According to the statistical analysis in this paper, the proposed circuit shows higher resilience to security attacks and reverse engineering attacks. The above mentioned three features are used to design a more reliable and secure PUF. The novelty in the proposed circuit is creating multiple delay output lines. Instead of directly providing the challenge bits to the circuit, they are xored differently at each MUX stage creating a different delay output line at each response. Thus by increasing the randomness and unpredictability of response.

CHARLES HERDER et.al [1]: The mentioned paper starts its discussion with two primary applications of PUF. they are cost of authentication must be low and security in key generation. PUF is broadly classified into two main categories namely strong PUF and weak PUF. Generally, authentication is preferably done by strong PUF and key storage is done by weak PUF's.

The below mentioned features are the key features of a weak PUF:

- The total number of challenge response pairs are less
- The response obtained from weak PUF is robust for different environmental conditions and stable and the readings of the response are same even if the challenge is provided multiple number of times.
- The responses generated are highly unpredictable and purely depends upon the variations in the manufacturing of devices
- It is almost impossible to design two different devices with same physical digital signature
- Ring oscillator PUF and SRAM PUF are the two examples of weak PUF.

The below mentioned features are the key features of a strong PUF:

- The total number of challenge response pairs are large. They are large enough so that attacker cannot enumerate all the possible challenge response pair in given time.

- The response obtained from strong PUF is robust for different environmental conditions and stable and the readings of the response are same even if the challenge is provided multiple number of times.
- Even if attacker has a list of challenge response pairs, it is hard to predict the response of randomly and newly chosen challenge
- It is almost impossible to design two different devices with same physical digital signature
- Attacker may be revealed with only the response but not about the internal functionality of the device
- Optical PUF and arbiter PUF are the examples of strong PUF.

YINGJIE LAO et.al [8]: In this paper they have proposed a novel reconfigurable PUF. they have approached in two major ways one is using PUF with LFSR and other is using PUF with hash function. The effectiveness of the proposed reconfigurable PUF is demonstrated in their experimental results. This demonstration is done by using intrachip variations and interchip variations. Also several security methods are proposed in this papers using reconfigurable PUF. They have used a different perspective to judge the reliability concept in PUF. Mathematical analysis of the proposed highly secure novel PUF is done in this paper. Calculations of re-configurability are done on challenge LFSR, output recombination, MUX/DEMUX, reconfigurable feed-forward and challenge hash. All these variations are compared in terms of minimum, maximum and average comparisons.

SRINIVAS DEVADAS et.al [9]: This paper is mainly focused on how PUF authentication is done for RFIDs. The main requirements of the RFIDs are security and cost. PUF can fulfill these two requirements for RFIDs. The experimental and testing results of this paper demonstrate that PUF is capable to securely authenticate RFIDS. They have also highlighted the advantages of RFIDs based on PUF in different applications like security and anti-counterfeiting. They have calculated the code distance based on intrachip and interchip variations. They have compared the results of PUF based RFIDs with the results from cryptographic and track and trace operations. PUF based RFIDs provide the advantage of low cost and minimal overheads. They have fabricated the RFID on 0.18ų technology and demonstrated the results.

KOTA FRUHASHI et.al [10]: This paper mainly concentrates on hamming distance of the PUF. Hamming distance is used check the performance parameters of PUF like reliability, uniqueness, randomness etc. in this paper they have calculated the hamming distance using binomial distribution. they also have calculated the standard deviation by approximating the hamming distance with normal distribution. In this paper they proposed novel architecture of arbiter PUF which utilizes RG-DTM (response generation according to delay time measurement). They have generated a 256-bit response using arbiter PUF and calculated the uniqueness of this PUF using hamming distance. The novel PUF proposed in this paper is evaluated using standard deviation. The standard deviation of the above proposed PUF is greatly improved by from 8.45 to 31 when compared with conventional PUF.

SIARHERI S. ZALIVAKA et.al [11]: In this paper, the main focus is on what are the challenges in the implementation of delay based PUF. The main performance parameters of the PUF are reliability and uniqueness. the main problem while implementation is either we get a poor reliability or the PUF is vulnerable to high predictability. Poor reliability is caused due to variation in environmental conditions during the implementation of PUF. Therefore, during implementation always, a tradeoff is created between the unpredictability and reliability. Due to low reliability arbiter PUF always suffers from machine learning attacks. To overcome these problems a novel method in implementation of PUF on FGPA is given in this paper. In this paper they have removed weak challenge bits and improvised the strong challenge bits by obfuscation techniques. this increases the resilience of PUF against machine learning attacks.

JING YE et.al [12]: In this paper a novel PUF called obfuscation PUF is proposed. In standard PUF one of the main in implementation is the modelling attack. To make the PUF more resilience towards such attacks a novel PUF called obfuscation PUF (OPUF) is proposed in this paper. In OPUF the challenge bits are first sent to obfuscation cell first and then they are sent to different MUX stages. In this paper different possible obfuscation cells are proposed. By doing this we increase factors like non determinacy and computational complexities. Increasing non-determinacy and computational complexity increases the unpredictability between challenges and responses .in this way PUF is made resistant towards attacks. The experimental results and theoretical analysis in this paper shows that the OPUF is has good stability and randomness.

YANSONG GAO et.al [13]: This paper concentrates on the statistical analysis of obfuscation PUF. In this paper they proposed an architecture which is hard to clone. the proposed circuit is also light weight and secure PUF. in this paper they have discussed about primary obfuscated PUF. Then they discussed about the uniqueness of OPUF and about collisions and patterns. They have calculated the predictions based on hamming distance. Followed by challenge pattern control, challenge recovery, authentication protocol of challenge response pairs. A completely statistical analysis on OPUF is done. attacks based on model building are also discussed in this paper.

JAMES B. WENDT et.al [14]: In this paper hardware obfuscation is done on the basis of PUF. Initially they gave a basic overview of PUF. Then discussed about arbitrary logic replacement. Followed by programmable fabric configuration then how to stabilize the standard PUF. they discussed the logic of signal path in obfuscation. Using PUF inputs for obfuscation completely hides the replaced logic. They specially mentioned two logics one is using PUFs and reconfigurable logics in direct replacement of arbitrary logics and the other is signal path obfuscation. The experimental results in this paper prove that PUF can successfully obfuscate the circuit functionality. They have also provided algorithms for each new technique proposed in the paper. Attacks and analysis of OPUF is also discussed in this paper.

SHIBANG LIN et.al [15]: This paper con concentrates on designing PUF using cascade current mirrors. Implementation of PUF architecture is done by cascading a NMOS transistor as load. The output impedance of the proposed circuit is great. Based on this, a small mismatch of current gives a large amplified output. In this architecture, the area required per bit response is two NMOS transistors, first transistor acts as a load in current mirror and other acts as selecting switch. Post stimulation is done UMC 65nm CMOS technology and the average per bit response is 5.47µm2.

CHAPTER 3

RESEARCH METHODOLOGY:

Physically unclonable functions (PUF) have turned a new page in hardware security. The input bits of PUF are called challenges and output bits of PUF are called responses. Their mapping is popularly known as CRP pairs. The challenge bits are given to the PUF, they are randomized in the possible way depending upon the type of PUF and responses are obtained.

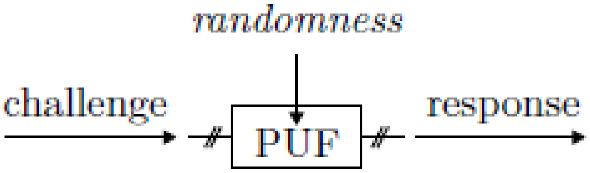


Fig 3.1: black box of PUF [17]

PUFs are used mainly for two major applications namely, key generation must be secure and authentication with low cost. Based on these two applications the PUFs designed from previous research works are categorized into two domains. they are

1. strong PUF

2. weak PUF.

The typical usage of strong PUF is authentication and key generation is done by weak PUFs. We shall about strong PUF and weak PUF in brief in our further discussion.

In other words, we can describe PUF as the black-box model of challenge response pairs. PUF is given with input challenge c and the output response would be r. the relation between challenge and response is given by

$$r = f(c)$$

where f(.) gives the function between challenge and response.

We can say the mentioned black-box model is appropriate to describe the PUF because the parameters of f(.) are unknown and hidden from external users. f(.) represent the manufacturing variations that occur internally in the PUF and are used to generate a set of CRPs which are unique. Parameters of f(.) can be of any type as discussed in introduction. The security of PUF relies on the parameters of f(.). as the difficulty level in measuring and estimating the parameters of f(.) increases, the security of PUF increases. Security also relies on difficulty in manufacturing two integrated circuits with same parameters of f(.).

PUF is differentiated into strong and weak PUF based on the domain f(.). In other words, we can say that a weak PUF can process has a limited number of CRPs and a strong PUF can process a large number of CRPs so that the determination and measurement of all the CRPs with in a limited period of time not possible.

3.1 WEAK PUF:

The basic implementation of PUF was started from weak PUFs. As we know that PUF can generate a unique finger print also called as digital signatures. Weak PUFs can provide us a digital signature which can be used for crypto graphic purposes. As the fingerprint remains invariant largely, a weak PUF can process only limited number of challenges.

Relating this to black box description provided above as there are limited number of input challenges, the domain of f(.) is limited. As we require same response for the given challenge ignoring environmental noise, the range of f(.) is also limited.

The following are few properties of the weak PUF:

- The total number of challenge response pairs are less
- The response obtained from weak PUF is robust for different environmental conditions and stable and the readings of the response are same even if the challenge is provided multiple number of times.
- The responses generated are highly unpredictable and purely depends upon the variations in the manufacturing of devices
- It is almost impossible to design two different devices with same physical digital signature
- Ring oscillator PUF and SRAM PUF are the two examples of weak PUF.

A simple example of weak PUF is the power on state of SRAM. Even though there is symmetry in SRAM cell, the variability in manufacturing gives a tendency to each cell in SRAM to either obtain ‘0’or ‘1’ in its power on state.

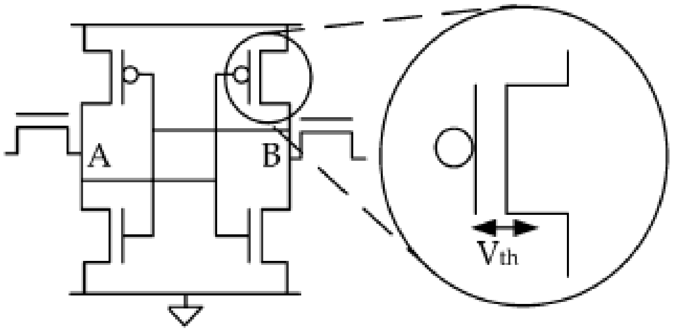


Fig 3.1.1: SRAM cell [1]

SRAM obtains ‘0’ or ‘1’ in a random nature across all the cells. The different responses in each cell are random and create digital fingerprint. In this case the challenge bit is always constant that is the power on state. The size of responses can be increase by increasing the number of cells in SRAM but still they all depends on manufacturing variability. SRAM is a typical example of weak PUF with only one CRP pair.

As the number of CRP pairs in weak PUF are limited. therefore, the obtained CRP must be kept in secret. They must not be revealed in any condition. If they are revealed to outer we lose the uniqueness of PUF. This the reason we use weak PUFs mostly for key generation and not for authentication. Once the key is generated from PUF it is used for cryptographic purposes like encryption and decryption.

3.2 STRONG PUF:

A strong PUF differs from weak PUF depending on the number of challenge response pairs. A strong PUF has a large number of CRP pairs. As the strong PUF has large number of CRP pairs, it does not require special cryptographic hardware for authentication. A strong PUF by itself can authenticate an integrated circuit without the requirement of any complicated cryptographic hardware. This is one of most primary advantages of PUF over other hardware security protocols.

The following the few key features of strong PUF:

- The total number of challenge response pairs are large. They are large enough so that attacker cannot enumerate all the possible challenge response pair in given time.

- The response obtained from strong PUF is robust for different environmental conditions and stable and the readings of the response are same even if the challenge is provided multiple number of times.
- Even if attacker has a list of challenge response pairs, it is hard to predict the response of randomly and newly chosen challenge
- It is almost impossible to design two different devices with same physical digital signature
- Attacker may be revealed with only the response but not about the internal functionality of the device
- Optical PUF and arbiter PUF are the examples of arbiter PUF

Weak PUF can also be used for authentication if it is paired with the hardware of cryptography. It is to be noted that security protocols of strong and weak PUF are different. In weak PUF the secret key must not be disclosed whereas in strong PUF there is no such compulsion.

There is one more additional restriction in the security module of strong PUF that is read out restricted access. This done to prevent the unauthorized access in to the PUF. to calculate the total enumerations of PUF, along with the CRPs we need to consider the readout time of the strong PUF also. If the response of PUF is faster the enumerations of PUF is also faster. In weak PUF only secret key is generated and rest security protocol is done cryptographic hardware but strong PUF does not have such hardware. Therefore, in order to rule out any unauthorized access this restriction is provided.

3.3 AUTHENTICATION PROTOCOL:

As discussed earlier, the input of strong PUF is challenge and output of PUF is response. Even if the adversary is provided with information of CRP pairs that is polynomial distribution of CRPs, the prediction of response to a new challenge is nearly impossible.

The mentioned is desired property of PUF but it also gives us new challenge. As told, the PUF is represented by a black box, even the server which is used for authentication is stored only with the previously obtained CRPs and cannot predict the response of new challenge.

Therefore, in PUF a different protocol is used for security and is different the system of cryptography which uses public and private key.

The below are steps to authenticate a client with PUF server:

- Initially manufacturing of PUF is done.
- The access of PUF is given to a particular server. Now the server generates a table with all the possible CRP pairs. These CRP pairs are stored in secret internal memory.
- Client is with PUF circuit.
- Now the client needs to submit a request of authentication to the particular server in which CRP pairs are stored.
- As server has the database of CRP pairs, it pucks up any known challenge and will send it to the client.
- Now the client is provided with a challenge and PUF circuit. Client provides input to the PUF circuit and will send generated output response to the server.

- The server verifies the received response from with the database of CRP pairs and highlights the CRP pair as used.

As the behavior of PUF is highly unpredictable, the CRP pairs must ne internally stored for future usage. The CRP pair can be used only for a single time, so the database of the CRP pairs must be large enough that it can last long or the server need to maintain a good communication with client to be authenticated so that the database can be recharged periodically.to reduce this problem of CRPs new protocols are being developed.

3.4 PERFORMANCE PARAMETERS OF PUF:

The below mentioned are the few performance parameters that are used to evaluate PUF:

1. INTRACHIP VARIATIONS:

When a same challenge is provided to same PUF under different environmental parameters, the number of bits that vary in output response of the PUF are defined as the intrachip variations. These variations are mostly represented in statistical distribution form. They measure the reproducibility of each PUF circuit.

2. INTERCHIP VARIATIONS:

When same challenge is provided to two different PUFs under same environmental conditions, the number of bits that vary in the output responses of the two PUFs are defined as inter chip variations. They are also mostly represented in statistical distribution form. They are used to measure the uniqueness of individual PUF.

3. HAMMING DISTANCE:

Hamming distance is the measure of similarity. It measures the number of identical in the respective bit positions. Hamming distance is used to measure the reliability of PUF. It is measured between the expected output and the output generated.

$$\mathrm{HD}(x,\ y) = \sum_{i=1}^{n} \left(x_i \oplus y_i\right)$$

Fig 3.4.1: Hamming Distance [16]

4. RELIABILITY:

It is calculated based on intrachip variations. P*intra* represent the probability that a particular bit in the response will flip when applied with randomly selected challenges for multiple times [2].

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

Fig 3.4.2: Reliability [2]

5. UNIQUENESS:

It is calculated from the interchip variations. P*inter* represents the probability that the bits generated by the same challenge for different PUF instances are different [2].

$$E(HD_{inter}) = P_{inter}$$
$$= E\left(\frac{2}{(K-1)K}\sum_{i=1}^{K-1}\sum_{j=i+1}^{K}\frac{HD(R(i), R(j))}{L}\times 100\%\right).$$

Fig 3.4.3: Uniqueness [2]

6. RANDOMNESS:

Randomness represents the ability of the PUF to output ‘0’ or ‘1’ response with equal probability [2].

$$Randomness = 1 - |2P(R = 1) - 1|.$$

Fig 3.4.4: Randomness [2]

3.5 ARBITER PUF:

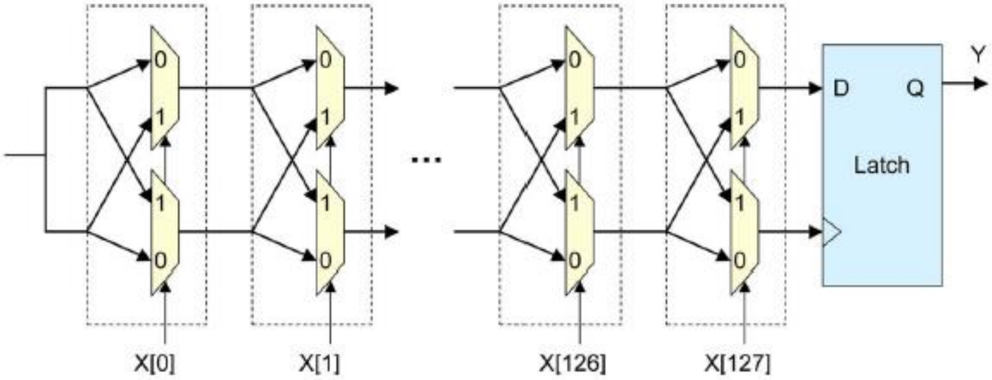


Fig 3.5.1: Arbiter PUF [1]

An arbiter PUF consists of N-stages of MUX. Each stage of MUX is terminated with an arbiter. The arbiter can be any latch or flip-flop. Here, in this paper I used D-latch as an arbiter. Each stage consists of two MUX. These MUX flip the path of the incoming signals. This flipping is done based on the challenge bit. If the challenge bit is ‘0’, a straight forward path is provided for the incoming signals. If the challenge bit is ‘1’ the path incoming signals is flipped. In this way we are creating two paths. When a rising edge is given to the input, the signal travels through two paths.

Now we organizing a race between these two paths. As we know each MUX component has different delay due manufacturing variations. Each path is added with different delay at each MUX component. These two are finally terminated at arbiter. Arbiter will output the signal which ever reaches it first. We cannot predict signal through which path arrives first as the delay added to the paths are due to manufacturing variations.

In this way we are generating an unpredictable response. To increase the length of response we can increase the number of MUX stages vertically. Therefore, a response of N-bit is generated for a N-bit challenge. In the mentioned figure we can see the standard linear arbiter MUX PUF. There are non-linear MUX PUF. In non-linear MUX PUF we add non-linearity to the paths to make the responses more unpredictable. Below we shall see few non-linear PUFs

3.5.1 FEED FORWARD MUX PUF:

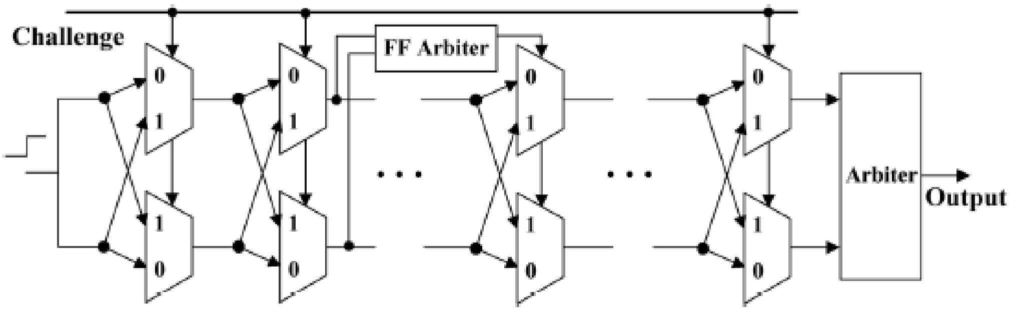


Fig 3.5.1.1: FF PUF [2]

In the feed forward MUX PUF extra feedforward paths are added to increase the randomness and unpredictability of PUF. the feed forward path is created by attaching the result of intermediate stage to the arbiter of feed forward path called FF arbiter. The result of the arbiter is provided as challenge bit to another stage of MUX. in this way we are creating a feed forward path and increasing randomness.

3.5.2 FEED FORWARD OVERLAP MUX PUF

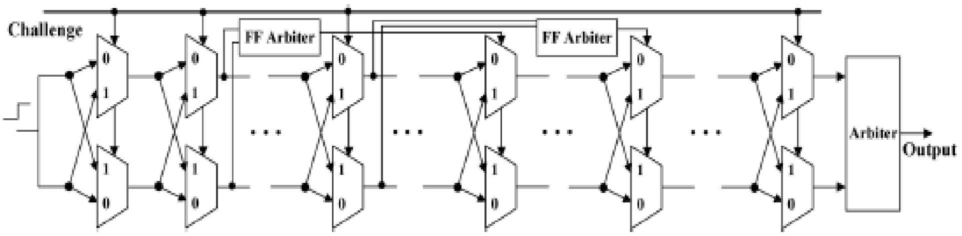


Fig 3.5.2.1: FFO PUF [2]

In feed forward overlap MUX PUF, between two feed forward paths there is at least one stage of overlap

3.5.3 FEED FORWARD CASCADE MUX PUF

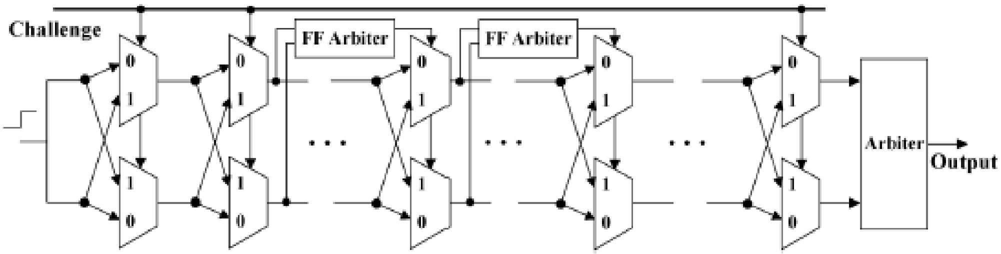


FIG 3.5.3.1: FFC PUF [2]

In feed forward cascade MUX PUF, at the very termination stage of one feed forward path another feed forward will be started.

3.5.4 FEED FORWARD SEPARATE MUX PUF

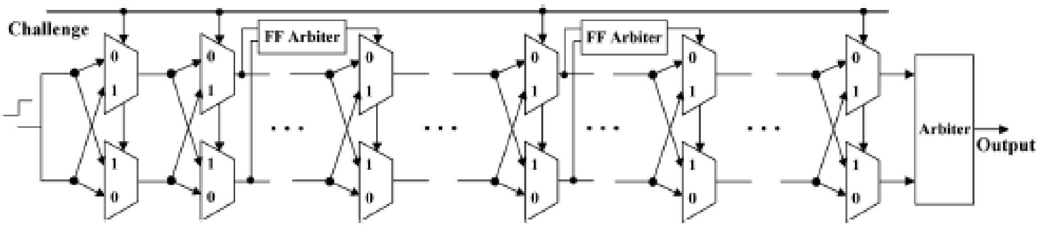


Fig 3.5.4.1: FFS PUF [2]

In feed forward separated MUX PUF, the is no relation between two feed forward paths. There is no overlapping or cascading.

3.5.5 MUX/DEMUX PUF

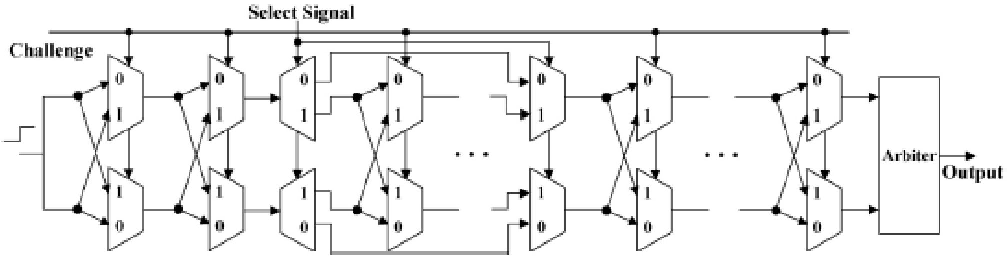


Fig 3.5.5.1: MUX/DEMUX PUF [2]

In this type of PUF we use DEMUX along with MUX as shown in the fig. it is a reconfigurable PUF. Here, we replace MUX in few stages with DEMUX and provide the output of DEMUX to two different stages of MUX away from each other.

3.5.6 MODIFIED FEED FORWARD MUX PUF

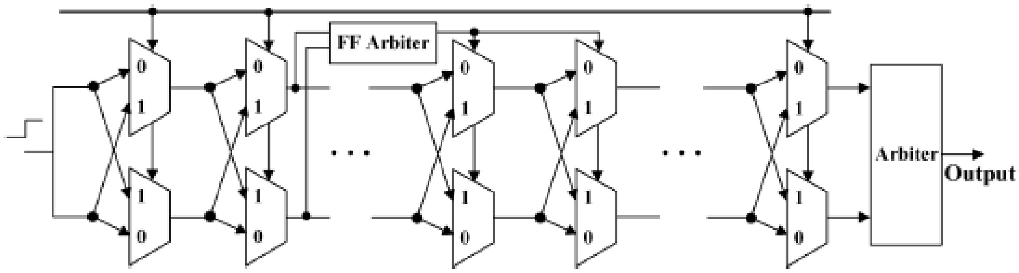


Fig 3.5.6.1: Modified FF PUF [2]

In normal feed forward MUX PUF, the output of FF arbiter is given as input to one of the other MUX stages. here in modified feedforward MUX the output of FF arbiter is not given single other MUX stage but it is given to multiple other MUX stages.

3.5.7 MODIFIED FEED FORWARD OVERLAP MUX PUF

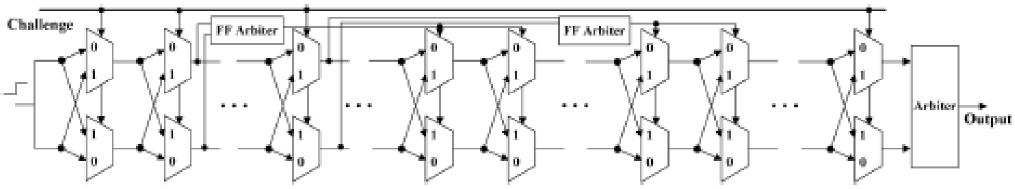


Fig 3.5.7.1: Modified FFO PUF [2]

Implementation is same standard overlap MUX PUF but the output of each FF arbiter is given as input to other multiple stages of MUX

3.5.8 MODIFIED FEED FORWARD CASCADE MUX PUF

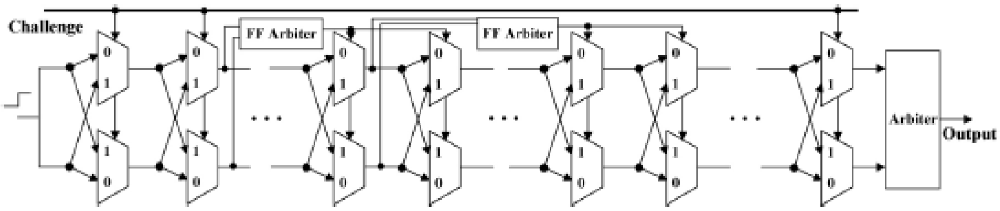


Fig 3.5.8.1: Modified FFC PUF [2]

Implementation is same standard feed forward cascade MUX PUF but the output of each FF arbiter is given as input to other multiple stages of MUX

3.5.9 MODIFIED FEED FORWARD SEPERATE MUX PUF

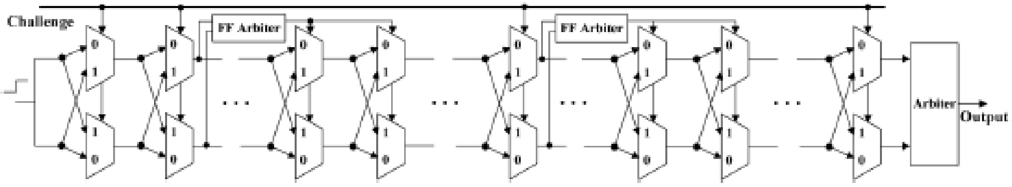


Fig 3.5.9.1: Modified FFS PUF [2]

Implementation is same standard feed forward separate MUX PUF but the output of each FF arbiter is given as input to other multiple stages of MUX

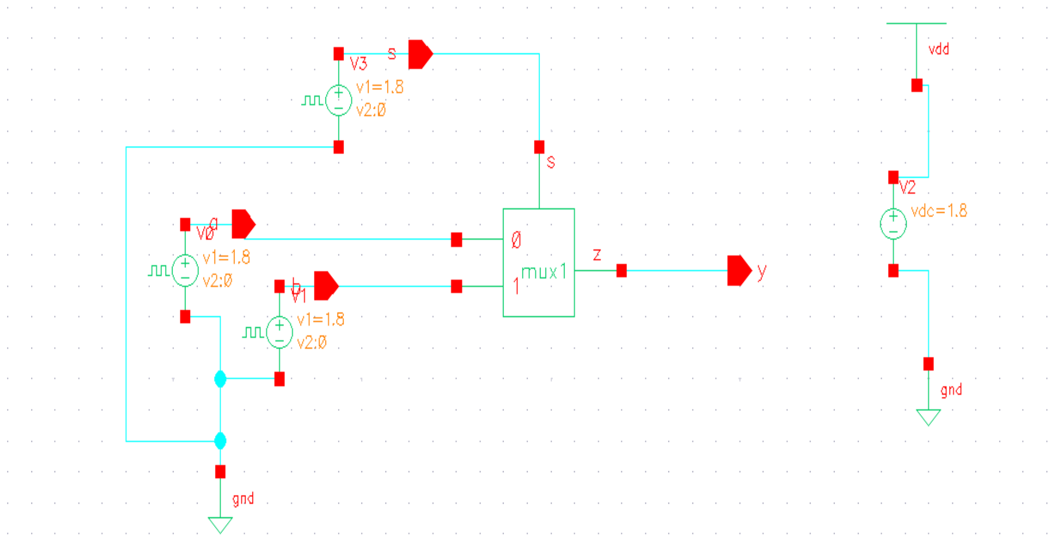
CHAPTER 4

WORKDONE

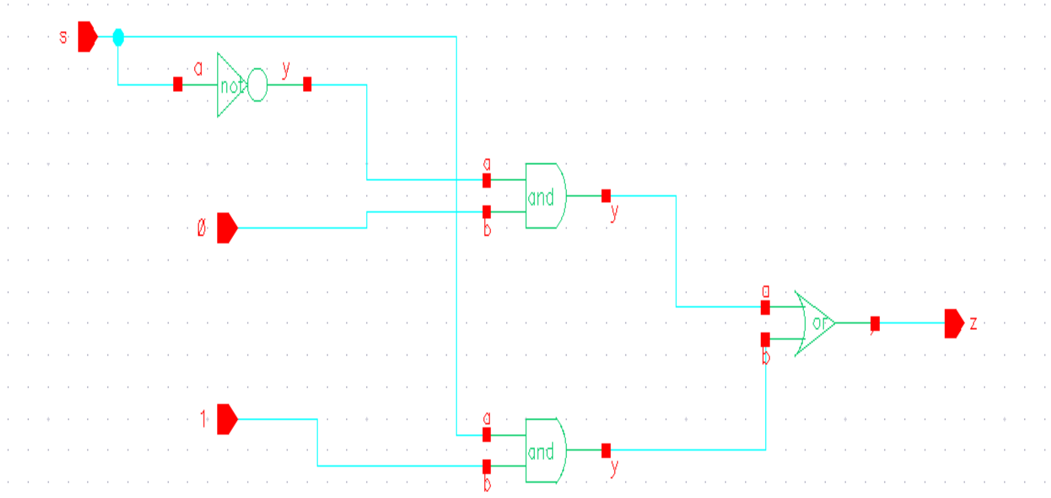
4.1 MUX:

As discussed above in each stage of arbiter PUF there two MUX. one of MUX in sequence 0-1 and the other MUX in the sequence of 1-0. I named the 0-1 MUX as MUX 1 and the 1-0 MUX as MUX 2 and the implementation of these two is shown below. The implementation is done in cadence virtuoso.

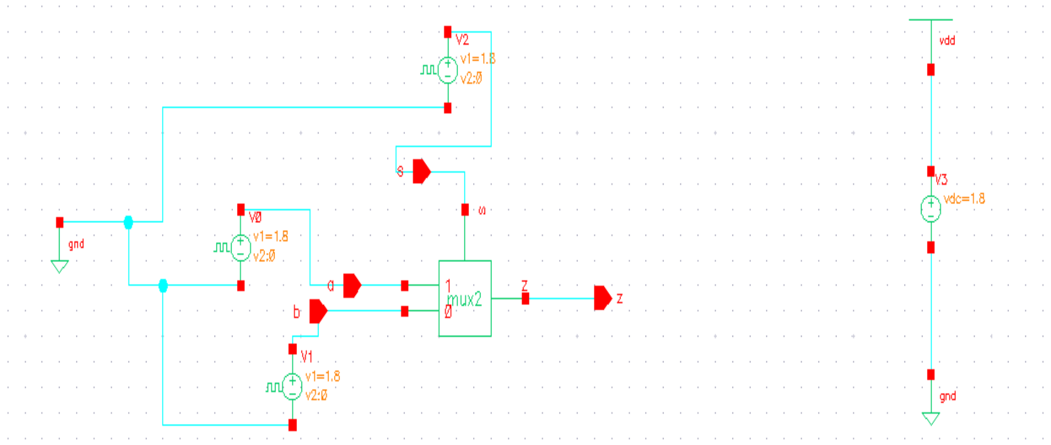
MUX 1:



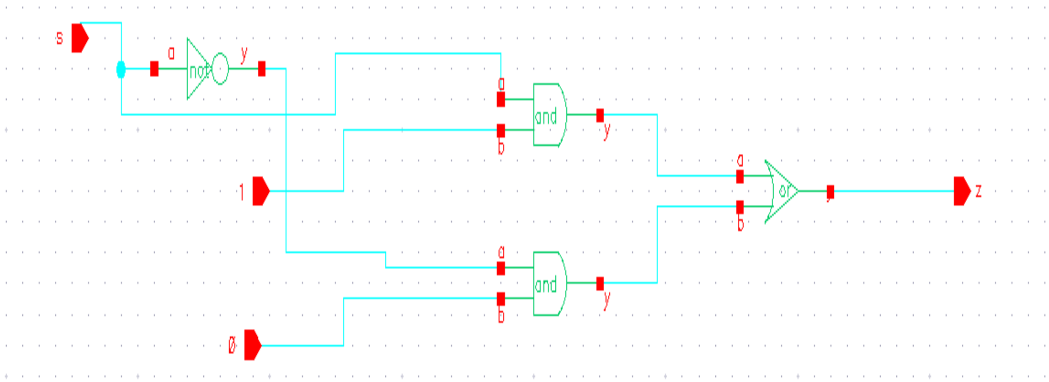
INTERNAL STRUCTURE OF MUX 1:



MUX 2:



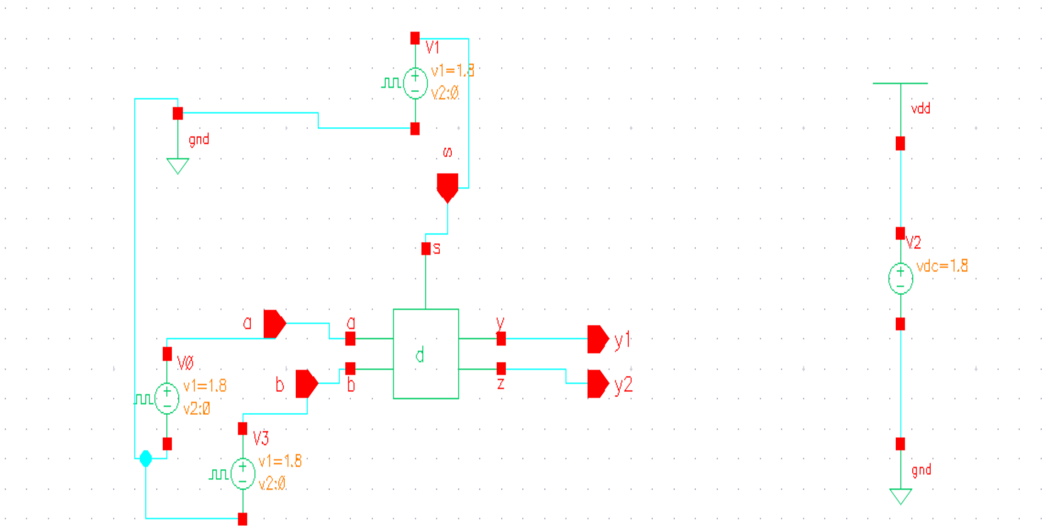
INTERNAL STRUCTURE OF MUX 2:



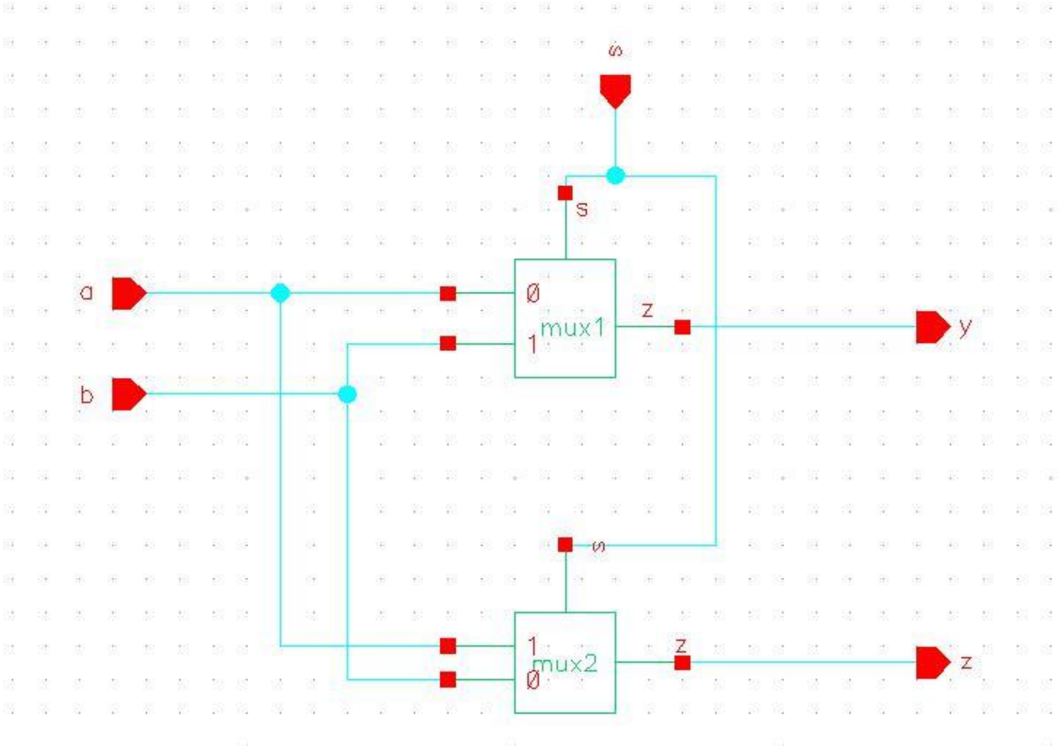
4.2 DELAY COMPONENT:

Combining the above designed two MUX. I have designed a delay component where the path of two are flipped based on the challenge bit.

DELAY COMPONENT:



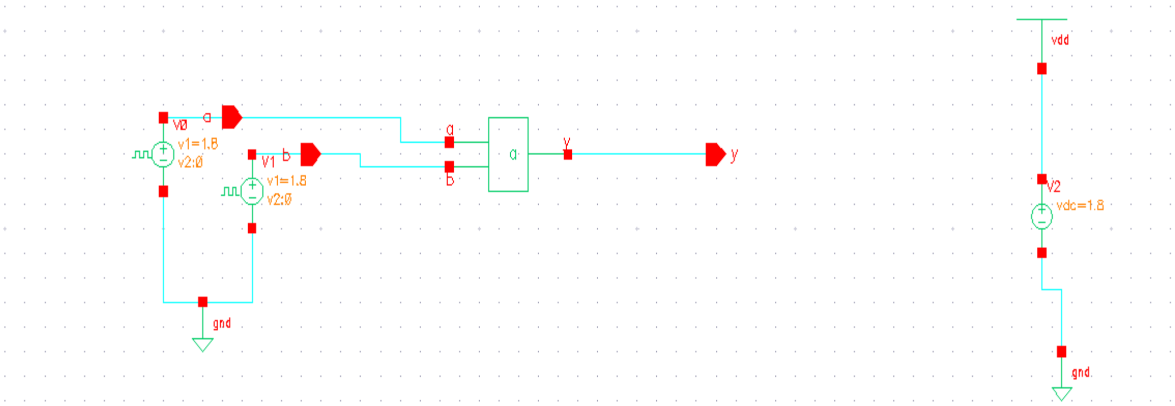
INTERNAL STRUCTURE OF DELAY COMPONENT:



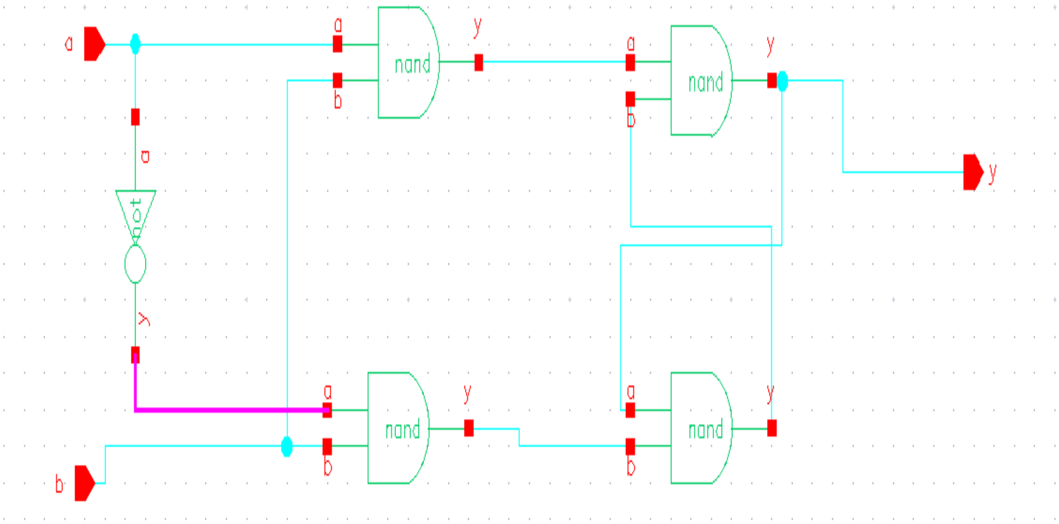
4.3 ARBITER:

As discussed above the arbiter can be any latch. Here, I used D-latch to implement the arbiter. Arbiter selects the first incoming path and generates output accordingly.

ARBITER:



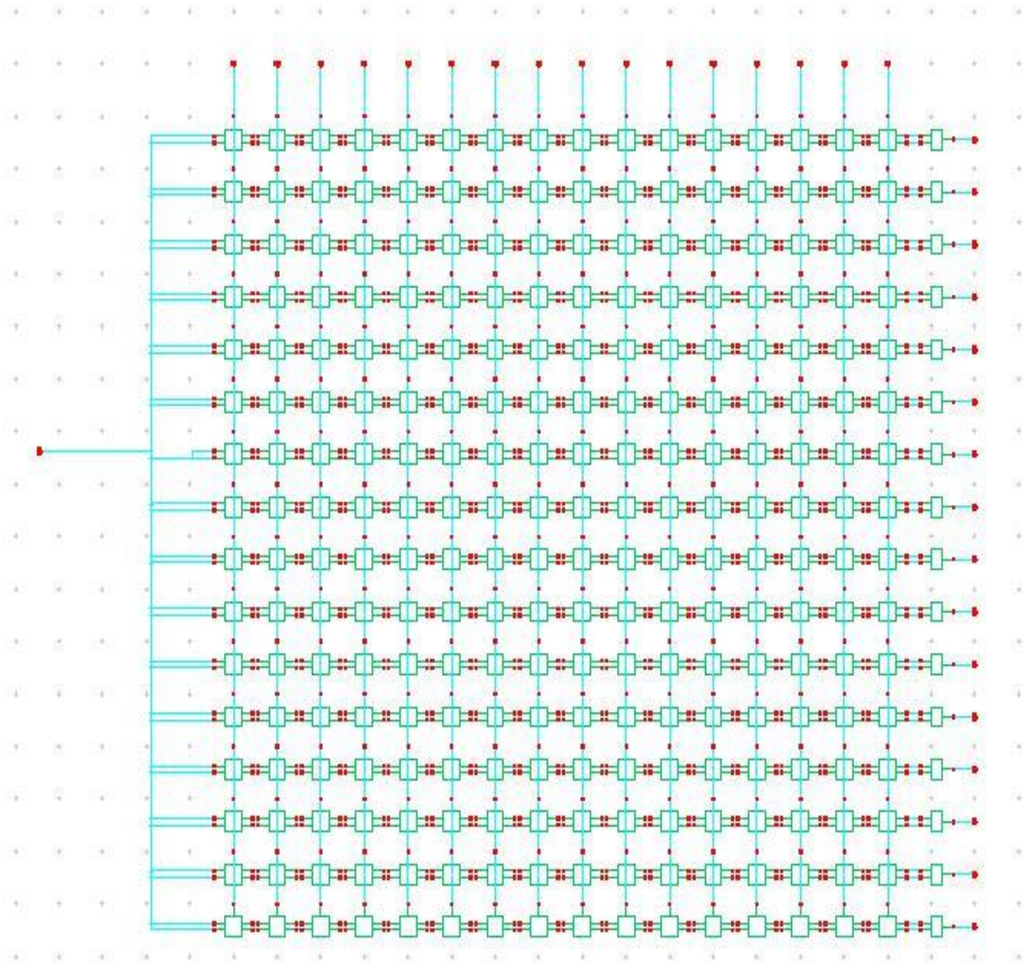
INTERNAL STUCTURE OF ARBITER:



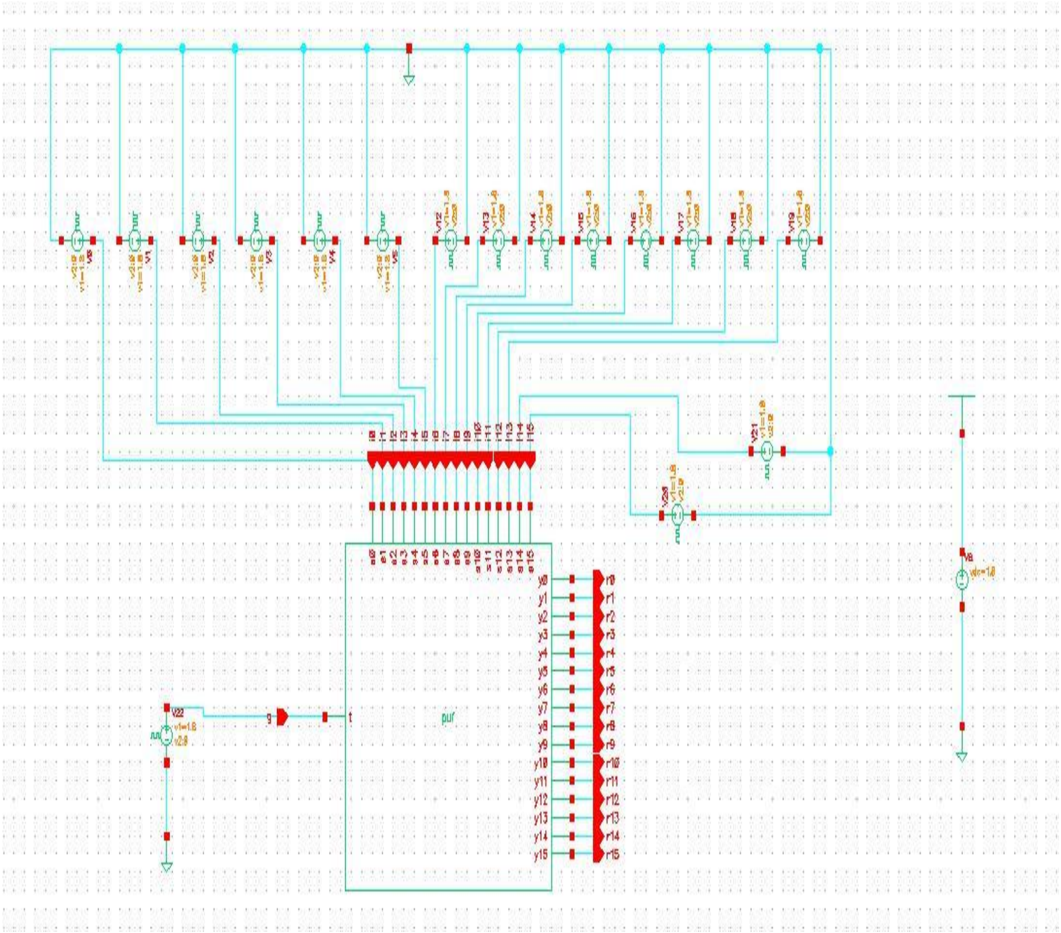
4.4 PUF 16 BIT:

Using the above components, I designed a 16bit PUF

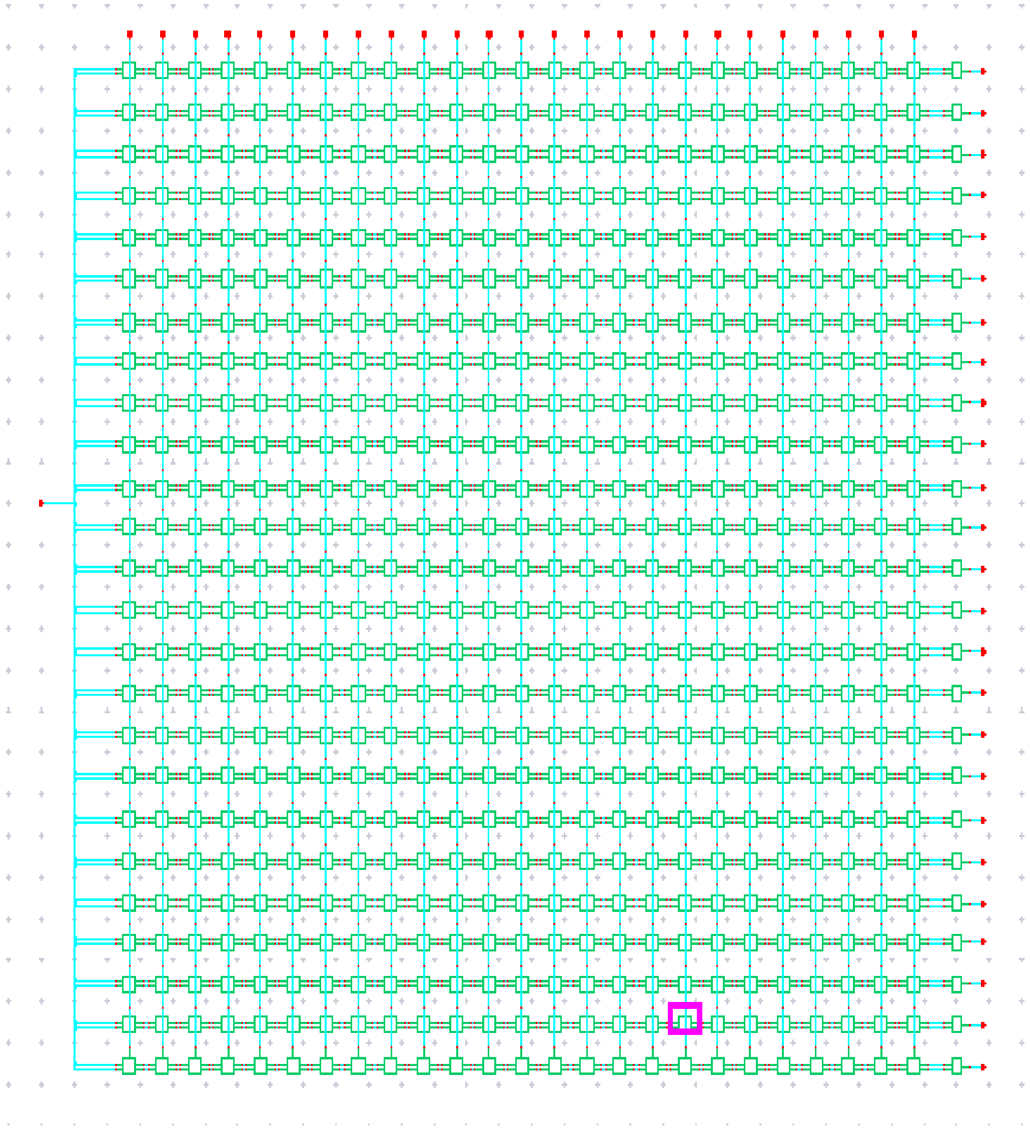
16 BIT PUF:



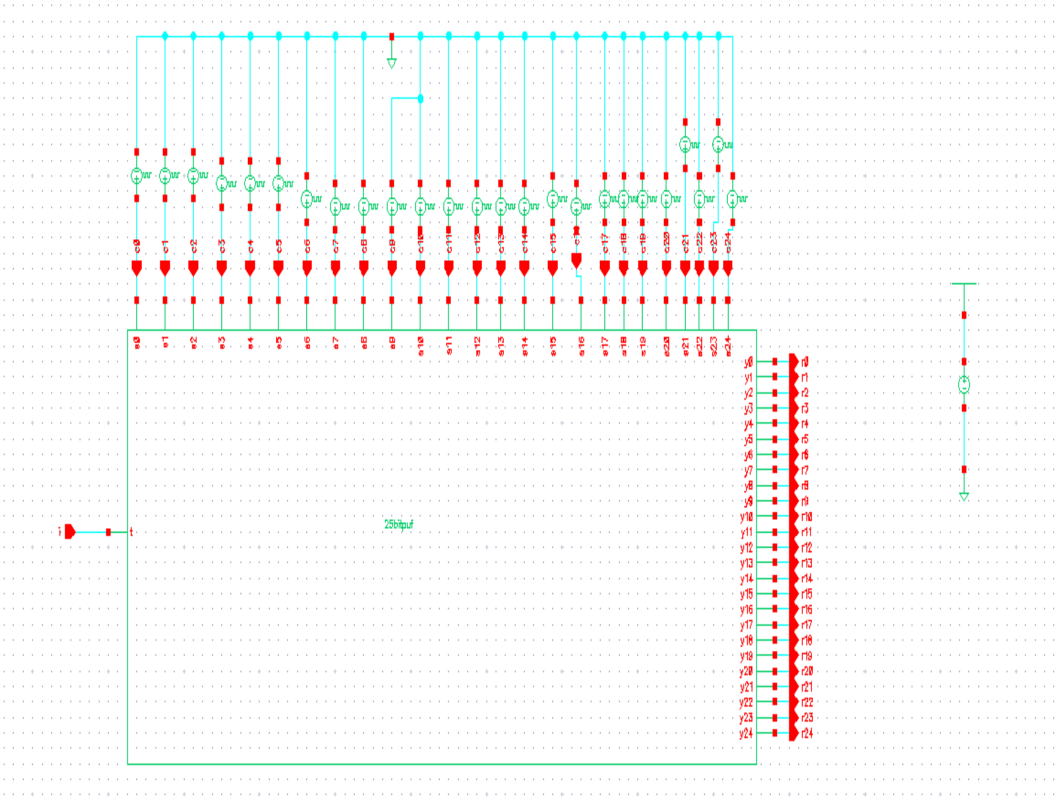
TEST BENCH OF 16 BIT PUF:



4.5 25 BIT PUF:



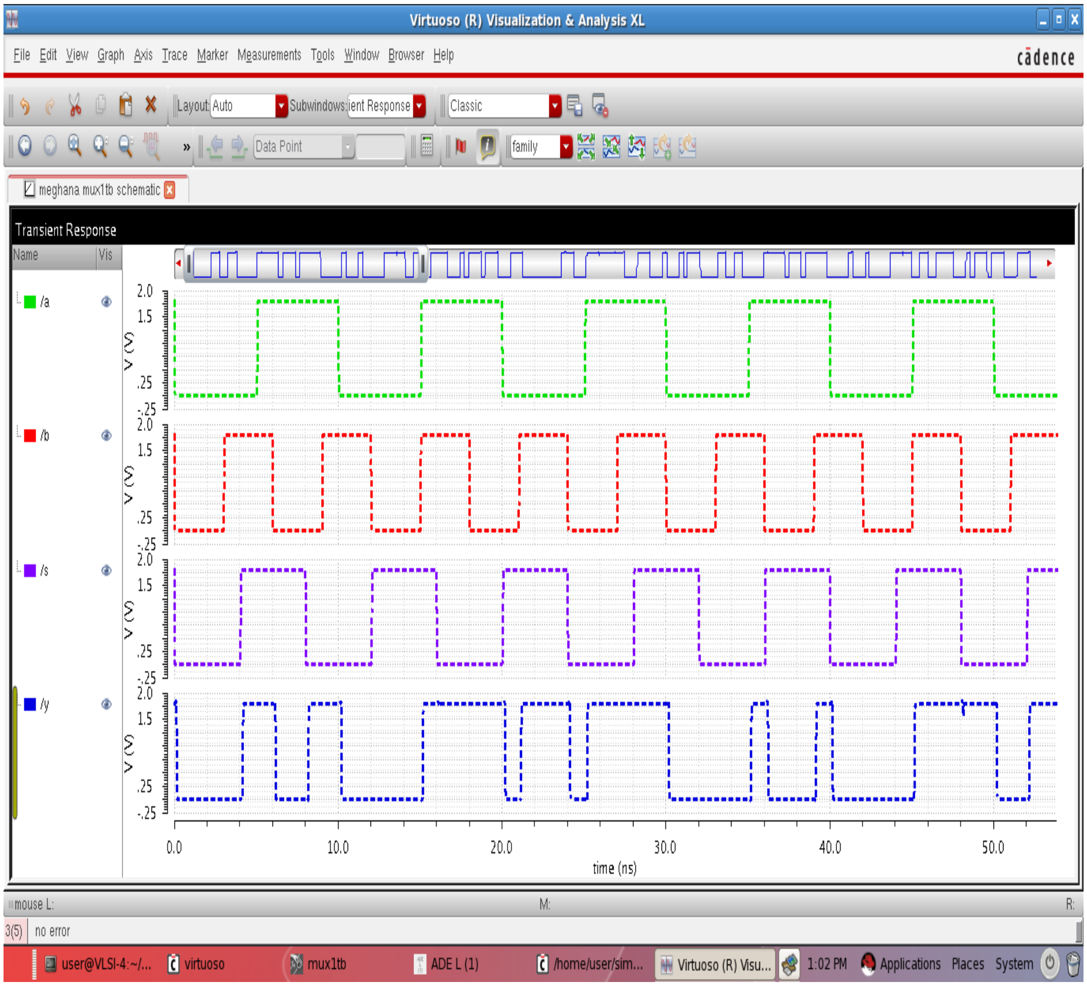
25 BIT PUF TEST BENCH:



CHAPTER 5

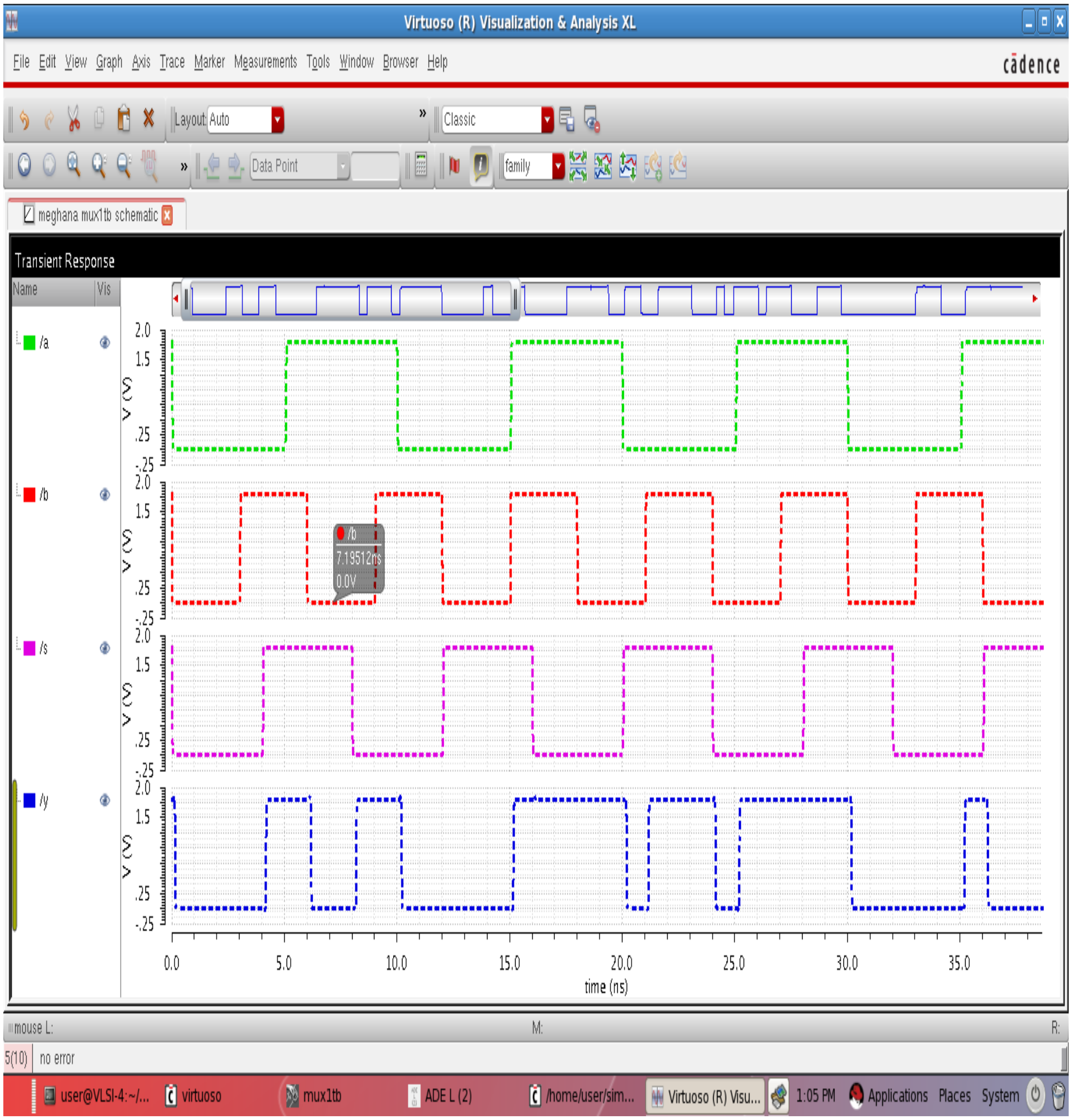
RESULTS AND DISCUSSION:

5.1 MUX 1:



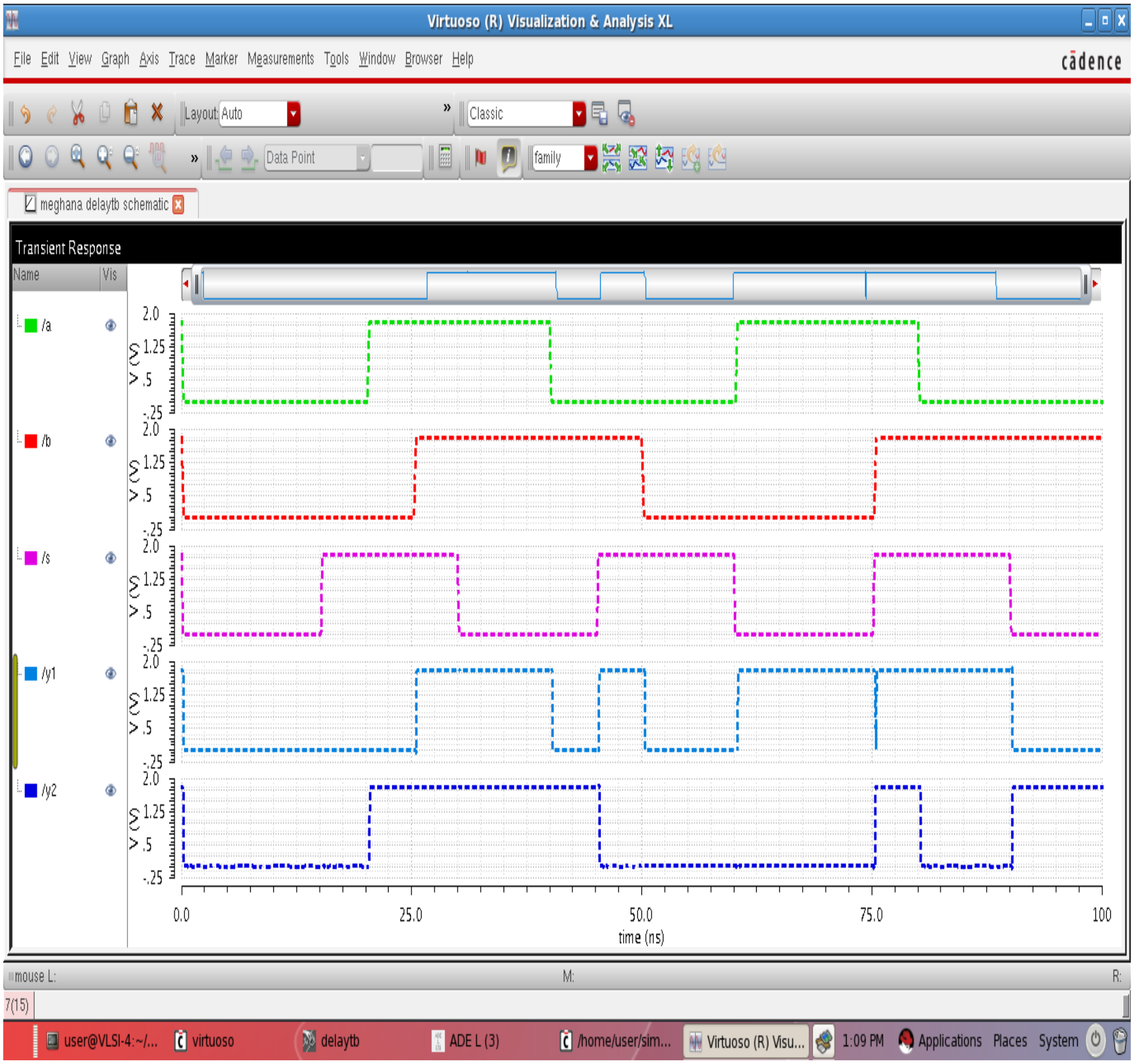
FroKm above graph we can see that when the select line ‘0’, first input will be selected. And when the select line ‘1’ second input will be selected.

5.2 MUX 2:



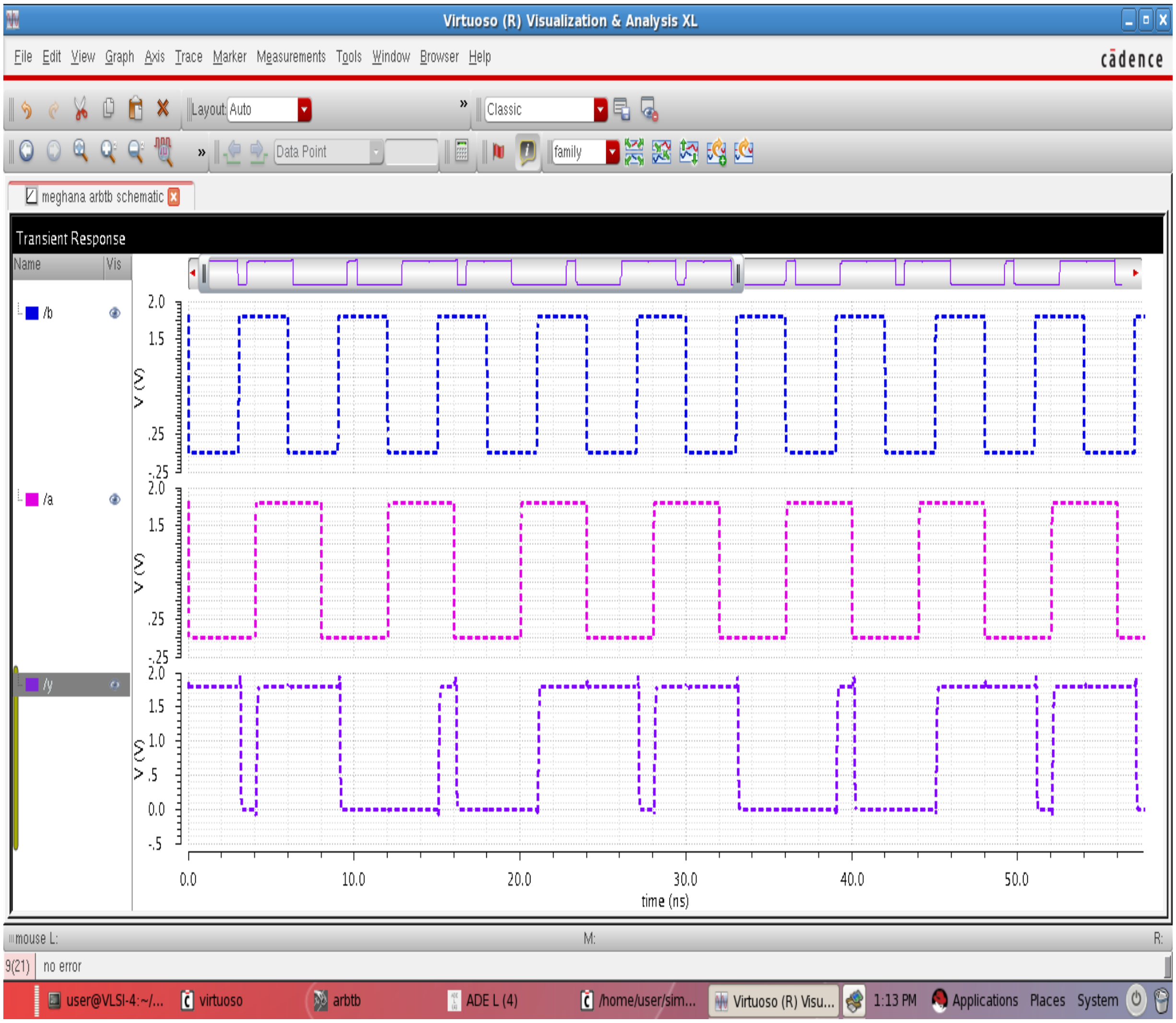
From the above we observe that when select line ‘0’, second input will be selected and when the select line is ‘1’, first output will be selected.

5.3 DELAY COMPONENT:



As discussed earlier, the input must me flipped depending upon the select line. From the above graph we can see that when the select line is ‘1’, the two paths are interchanged and when the select line is ‘0’, the straight forward path is provided for two inputs without any interchanging

5.4 ARBITER:



As already told, I have D-latch as the arbiter, the above results justify it. Whenever the clock is ‘0’, the output retains its previous states and whenever the clock is ‘1’, the input will be reflected in the output.

CHAPTER 6

CONCLUSION:

Physically Unclonable functions (PUF) are of various types depending on various manufacturing variabilities. In this thesis, Implementation of delay PUF on based on MUX is done. MUX PUF are basically of two types linear and nonlinear PUF. I have implemented linear PUF in two different stages one is 16 bit and other is 25 bit. From the above implementation we can determine different challenge response pairs (CRP). These challenge response pairs can be used either for authentication or secret key generation. Finally, Power analysis of both 16 bit and 25-bit linear delay based MUX PUF is done with

CHAPTER 7

FUTURE SCOPE:

Delay based MUX PUF basically depends on the randomness in the delay paths present in different stages of MUX. randomness can be increased by adding non linearity to these delay PUFs. Such PUFs are called nonlinear PUFs. The future scope of this thesis is, we can add non linearity to implemented linear delay based MUX PUF. Increasing the non-linearity makes PUF more reliable and unique. the performance of the linear and nonlinear PUFs can evaluated by parameters like reliability , randomness and uniqueness.

REFERENCES :

1. Herder, Charles, et al. "Physical unclonable functions and applications: A tutorial." *Proceedings of the IEEE* 102.8 (2014): 1126-1141
2. Lao, Yingjie, and Keshab K. Parhi. "Statistical analysis of MUX-based physical unclonable functions." *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems* 33.5 (2014): 649-662.
3. Avvaru, S. V., et al. "Estimating delay differences of arbiter PUFs using silicon data." *Proceedings of the 2016 Conference on Design, Automation & Test in Europe*. EDA Consortium, 2016.
4. Avvaru, SV Sandeep, et al. "Predicting Hard and Soft-Responses and Identifying Stable Challenges of MUX PUFs using ANNs."
5. Gassend, Blaise, et al. "Silicon physical random functions." *Proceedings of the 9th ACM conference on Computer and communications security*. ACM, 2002.
6. Lao, Yingjie, et al. "Reliable PUF-Based Local Authentication With Self-Correction." *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems* 36.2 (2017): 201-213.
7. Majzoobi, Mehrdad, Farinaz Koushanfar, and Miodrag Potkonjak. "Lightweight secure pufs." *Computer-Aided Design, 2008. ICCAD 2008. IEEE/ACM International Conference on*. IEEE, 2008.
8. Lao, Yingjie, and Keshab K. Parhi. "Reconfigurable architectures for silicon physical unclonable functions." *Electro/Information Technology (EIT), 2011 IEEE International Conference on*. IEEE, 2011.
9. Devadas, Srinivas, et al. "Design and implementation of PUF-based" unclonable" RFID ICs for anti-counterfeiting and security applications." *RFID, 2008 IEEE International conference on*. IEEE, 2008.

10. Fruhashi, Kota, et al. "The arbiter-PUF with high uniqueness utilizing novel arbiter circuit with Delay-Time Measurement." *Circuits and Systems (ISCAS), 2011 IEEE International Symposium on*. IEEE, 2011.
11. Zalivaka, Siarhei S., Alexander A. Ivaniuk, and Chip-Hong Chang. "FPGA implementation of modeling attack resistant arbiter PUF with enhanced reliability." *Quality Electronic Design (ISQED), 2017 18th International Symposium on*. IEEE, 2017.
12. Ye, Jing, Yu Hu, and Xiaowei Li. "OPUF: Obfuscation logic based physical unclonable function." *On-Line Testing Symposium (IOLTS), 2015 IEEE 21st International*. IEEE, 2015.
13. Gao, Yansong, et al. "Obfuscated challenge-response: A secure lightweight authentication mechanism for PUF-based pervasive devices." *Pervasive Computing and Communication Workshops (PerCom Workshops), 2016 IEEE International Conference on*. IEEE, 2016.
14. Wendt, James B., and Miodrag Potkonjak. "Hardware obfuscation using PUF-based logic." *Proceedings of the 2014 IEEE/ACM International Conference on Computer-Aided Design*. IEEE Press, 2014.
15. Lin, Shibang, et al. "A low power and compact physical unclonable function based on the cascode current mirrors." *Circuits and Systems (APCCAS), 2016 IEEE Asia Pacific Conference on*. IEEE, 2016
16. Sadr, A., and M. Zolfaghari-Nejad. "Weighted Hamming distance for PUF performance evaluation." *Electronics Letters* 49.22 (2013): 1376-1378
17. Schuster, Markus. "Enhanced physical unclonable function structures in mixed-signal MOS technology." (2014).