

PERFORMANCE ANALYSIS OF AN EFFICIENT VLSI ARCHITECTURE USING GNRFET TECHNOLOGY

Submitted in partial fulfilment of requirements for the award of

Bachelor of Engineering in

Electronics and Communication Engineering

by

ANANTHALAKSHMI P (39130022)

SINDHUJA JS (39130429)



DEPARTMENT OF ELECTRONICS AND COMMUNICATION ENGINEERING

SCHOOL OF ELECTRICAL AND ELECTRONICS

SATHYABAMA

**INSTITUTE OF SCIENCE AND TECHNOLOGY
(DEEMED TO BE UNIVERSITY)**

Accredited with Grade "A" by NAAC

JEPPIAAR NAGAR, RAJIV GANDHI SALAI, CHENNAI – 600119

April – 2023



SATHYABAMA

INSTITUTE OF SCIENCE AND TECHNOLOGY

(DEEMED TO BE UNIVERSITY)

Accredited "A" Grade by NAAC | 12B Status by UGC | Approved by AICTE

www.sathyabama.ac.in

DEPARTMENT OF ELECTRONICS AND COMMUNICATION ENGINEERING

BONAFIDE CERTIFICATE

This is to certify that this Project Report is the bonafide work of ANANTHALAKSHMI P (39130022) and SINDHUJA JS (39130429) who carried out the project entitled "A Reconfigurable SRAM Based CMOS PUF with Challenge to Response Pairs" under our supervision from Aug 2022 to Oct 2022.

Internal Guide

Dr. MATHAN N., M.Tech., Ph. D
Assistant Professor

Head of the Department

Dr.T.RAVI M.E., Ph.D.

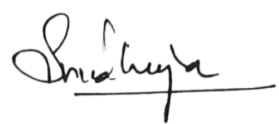
Submitted for Viva voce Examination held on _____

Internal Examiner

External Examiner

DECLARATION

We, ANANTHALAKSHMI P (39130022) and SINDHUJA JS(39130429) hereby declare that the Project Report entitled “**PERFORMANCE ANALYSIS OF AN EFFICIENT VLSI ARCHITECTURE USING GNR FET TECHNOLOGY**” done by us under the guidance of Dr. MATHAN N., M.Tech., Ph.D, Assistant Professor is submitted in partial fulfillment of the requirements for the award of Bachelor of Engineering degree in Electronics and Communication Engineering.

1. 
2. 

DATE:15.04.23

PLACE: CHENNAI

SIGNATURE OF THE CANDIDATES

ACKNOWLEDGEMENT

We are pleased to acknowledge our sincere thanks to Board of Management of **SATHYABAMA** for their kind encouragement in doing this project and for completing it successfully. We are grateful to them.

We convey our thanks to **Dr.N.M.NANDHITHA M.E.,Ph.D.**, Dean, School of Electronics and Communication Engineering and **Dr.T.RAVI M.E., Ph.D.** Head of the Department, Department of Electronics and Communication Engineering for providing me necessary support and details at the right time during the progressive reviews.

We would like to express our sincere and deep sense of gratitude to our Project Guide **Dr.MATHAN N., M.Tech., Ph.D** for his valuable guidance, suggestions and constant encouragement paved way for the successful completion of our project work.

We wish to express our thanks to all Teaching and Non-teaching staff members of the Department of **Electronics and Communication Engineering** who were helpful in many ways for the completion of the project.

ABSTRACT

Advancements in digital electronics are strongly linked to technology such as quality adjusted microprocessor prices, memory capacity, sensors and even the number and size of pixels in digital cameras. Digital electronics has contributed to world economic growth in the late twentieth and early twenty-first centuries. Moore & amp law describes a driving force of technological and social change, productivity and economic growth. The most important prime mover of low power research and design is our convergence to a mobile society. We are moving from desktops to laptops to handhelds and smaller computing systems. With this profound trend continuing, and without a matching trend in battery life expectancy, the lower power issues will have to be addressed. This entails that low power tools and methodologies have to be developed and adhered to. The current trends will eventually mandate low power design automation on a very large scale to match the trends of power consumption of today's integrated chips. Because the suggested PUF contains many CRPs in addition to the small space and quick operating speed that are advantages of the standard SRAM structure, it can be used in a larger variety of applications as a CRP PUF. In this project, initially a benchmark has been created by depicting the digital designs using conventional CMOS device. Performance will be measured by considering the parameters of VLSI such as power, delay, power delay product etc. In the next phase, the designs will be carried out in GNRFET and it will found that GNRFET outperform the conventional MOSFET designs in terms of performance metrics. In the above case, conventional model of GNRFET is used for the designs. However, the performance of the designs can be further improved by shrinking the size of the device which will be more efficient and reliable that can be used for low power applications and high-end real-time processors.

CHAPTER No.	TITLE	PAGE No.
	ABSTRACT	V
	LIST OF FIGURES	IX
	LIST OF TABLE	IX
	LIST OF SYMBOLS AND ABBREVIATIONS	XII
1	INTRODUCTION	1
	1.1 SRAM	1
	1.2 INTRODUCTION OF MOS TECHNOLOGY	3
	1.3 MOSFET BASED SRAM CELL DESIGN PROBLEMS	5
	1.4 PERFORMANCE METRICS OF SRAM CELL	6
	1.4.1 SNM	6
	1.4.2 POWER AND DELAY	7
	1.4.3 POWER DELAY PRODUCT	7
	1.5 CMOS TECHNOLOGY	7
	1.5.1 NMOS TECHNOLOGY	9
	1.5.2 PMOS TECHNOLOGY	10
	1.6 PUF TECHNOLOGY	11

2	LITERATURE SURVEY	13
	2.1 LITERATURE SURVEY	13
	2.2 LITERATURE SUMMARY	22
	2.3 PROBLEM DEFINITION	22
3	EXISTING SYSTEM	23
	3.1 OPERATING PRINCIPLE OF RECONFIGURABLE SRAM PUF	23
	3.2 IMPLEMENTATION OF OVERALL RECONFIGURABLE SRAM PUF SYSTEM	26
4	PROPOSED SYSTEM	31
	4.1 SIMULATION OF WAVEFORM USING MOSFET TECHNOLOGY	34
	4.2 DC ANALYSIS OF SRAM ARCHITECTURE USING GNRFET TECHNOLOGY	38
5	CONCLUSION AND FUTURE SCOPE	41

LIST OF FIGURES

FIGURE No.	TITLE	PAGE No.
1.1	SRAM CELL	2
1.2	MOS STRUCTURE	3
1.3	REGIONAL LINEAR	4
1.4	SATURATION REGION	5
1.5	DOUBLE GATE GNRFET	5
1.6	CMOS USING PULL AND PULL DOWN	9
1.7	NMOS DIAGRAM	9
1.8	PMOS DIAGRAM	10
1.9	PUF TECHNOLOGY	12
3.1	BASIC STRUCTURE OF CONVENTIONAL SRAM PUF	24
3.2	CONCEPTUAL STRUCTURE OF RECNFIGURABLE SRAM PUF UNIT	25
3.3	SCHEMATIC OF RECONFIGURABLE SRAM	26
3.4	ARCHITECTURE AND WAVEFORM OF SRAM PUF CHIP	27
3.5	OUTPUT FOR EXISTING ANALYSIS	29
4.1	THE STRUCTURE OF A MOSFET LIKE GNRFET	31
4.2	IV TRANSFER CHARACTERISTICS OF SYSMETRICAL N-TYPE AND P-TYPE GNRFET	33
4.3	SIMULATION RESULT FOR NOT GATE USING 32nm MOSFET TECHNOLOGY	34
4.4	SIMULATION RESULTS FOR AND GATE USING 32 nm MOSFET TECHNOLOGY	35
4.5	SIMULATION RESULTS FOR SRAM USING 16 nm GNRFET TECHNOLOGY	36

4.6	SIMULATION RESULTS FOR SRAM ARRAY ARCHITECTURE USING 16 nm GNRFET TECHNOLOGY	37
4.7	BUTTERFLY CURVE OF GNRFET BASED SRAM ARCHITECTURE IN RETENTION MODE	38
4.8	BUTTERFLY CURVE OF GNRFET BASED SRAM ARCHITECTURE IN ACCESS MODE	38
4.9	BUTTERFLY CURVE OF GNRFET BASED SRAM ARCHITECTURE IN WRITE MODE	39

LIST OF TABLES

3.1	ANALYSIS FOR PERFORMANEOF MOSFET	30
4.1	DEVICE PARAMETERTS OF GRAPHINE NANORIBBON FIELD EFFECT TRANSISTOR	32
4.2	ANALYSIS FOR PERFORMANE OF GNRFET USING 130nm	39
4.3	ANALYSIS FOR PERFORMANE OF GNRFET USING 16nm	40

LIST OF SYMBOLS AND ABBREVIATIONS

SRAM	STATIC RANDOM ACCESS MEMORY
CMOS	COMPLEMENTARY METAL OXIDE SEMICONDUCTOR
PUF	PHYSICALLY UNCLONABLE FUNCTION
BER	BIT ERROR RATE

CHAPTER 1

INTRODUCTION

Due to the development of internet of things (IoT) devices in applications like mobile and wearable computing, autonomous vehicles, and sensible grids, communication has been incorporated into many aspects of daily life. Building robust is essential because adversarial attacks, which are used by malicious producers, are becoming more sophisticated. According to Kerkhof's principle, secret random keys are a crucial component of authentication algorithms generated via a true random vary generator (TRNG). The low cost, ultra-small and low power blessings of CMOS technology make silicon PUFs appropriate as secret key generators in IoT. A powerful PUF has a huge CRP space that will rise exponentially with the equivalent area, in contrast to a poor PUF that has a CRP space that scales linearly with chip area. A system with limited CRP space could need to make up for possible applicants who might require more overhead.

1.1 SRAM

Starting from the design specification to the generation of mask layout, layout design of an integrated circuit has several processing steps which have to be carefully exercised. These steps include design of transistor level schematic, SPICE simulation of the circuit according to the designed W/L ratios of the individual transistors, drawing of the layout using a layout editor, design rule check, parasitic extraction and final simulation and verification. These all- processing methods are inevitable for the error free operation of chip and similar methodology is followed for the design of 1 K-Byte SRAM IC. Basic building block of the SRAM is SRAM cell which stores one bit data. Using common bit lines data can be read and written to the SRAM cell. SPICE, being an industry standard tool for circuit simulation and analysis, is used for the simulation and analysis of SRAM cell and subsequently for the whole design. Pre-charge circuit, sense amplifier and read-write circuits complete the one SRAM memory. The memory is arranged in row- column matrix which facilitates easy addressing of memory bits and also provides design flexibility. Once the functionality of one memory cell array is proved it can be duplicated several times with minor design change in the I/O control circuitry.

Block diagram of the complete chip is shown in Figure (1.1). Six transistor SRAM

cells are organized into 8 blocks. The capacity of the SRAM cell is 1 Kbyte. To address all these locations total 10 address lines from A0 to A9 are used. Out of these, A0 to A2 are used as column address decoding lines while A3 to A9 are used for decoding the rows. Each row consists total 8 memory cells and constitute to form one byte. Thus, address lines address each byte not each bit.

Each block is comprised of 128 rows and 8 columns. Thus, the total number of transistors required for memory cells are 6 transistors x 128 rows x 8 columns x 8 blocks = 49,152. Rows of each block are decoded using NOR based 7 x 128 decoder. Total 1024 transistors are required for this circuit. Row decoder outputs are connected to each row of each block. Similarly, each block is selected by the 3 x 8 column decoder. This requires total 32 transistors.

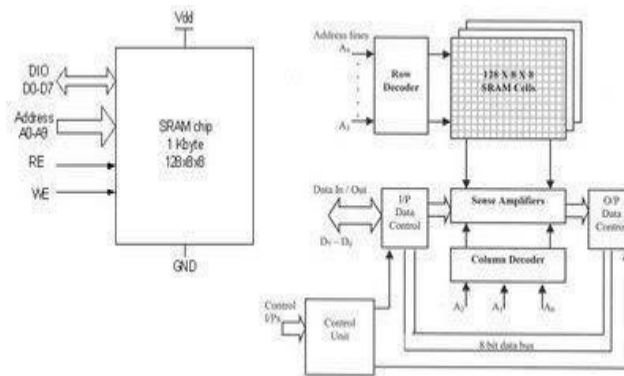


Fig 1.1: SRAM Cell

When sophisticated semiconductor and communication technologies were being developed in the 1970s, VLSI had its start. A VLSI device serves as the microprocessor. Prior to the development of VLSI technology, the majority of ICs could only carry out a finite number of tasks. A CPU, ROM, RAM, and other glue logic may be found in an electronic circuit. All of these may be incorporated into a single chip thanks to VLSI. Over the past few decades, the electronics sector has experienced tremendous expansion, mostly as a result of the quick development of large-scale integration technologies and system design applications. The use of integrated circuits (ICs) in high-performance computing, controls, telecommunications, image and video processing, and consumer electronics has increased significantly with the introduction of very large scale integration (VLSI) designs. Modern cutting-edge technologies provide end users an incredible range of applications, computing power, and portability. Examples include high resolution and low bit-rate video and cellular

communications. Rapid growth of this tendency is anticipated, with significant effects on VLSI design and system design.

1.2 An Introduction of MOS Technology

The transistor is the fundamental and most important part of an IC design. The MOSFET is a type of transistor that is employed in numerous applications. This transistor can be created similarly to a sandwich by sandwiching a semiconductor layer—typically a wafer, a slice from a single silicon crystal—a layer of silicon dioxide, and a layer of metal. The formation of transistors within the semiconductor material is made possible by these layers. SiO_2 is a good insulator and has a layer that is only 100 molecules thick. The gate parts of the transistors we utilize are made of polycrystalline silicon (poly), not metal. In high scale ICs, the polysilicon FET gate can almost entirely be replaced with metal gates. Because the SiO_2 below the gate is an insulator, polysilicon and metal FETs are sometimes referred to as IGFETs, or insulated gate FETs.

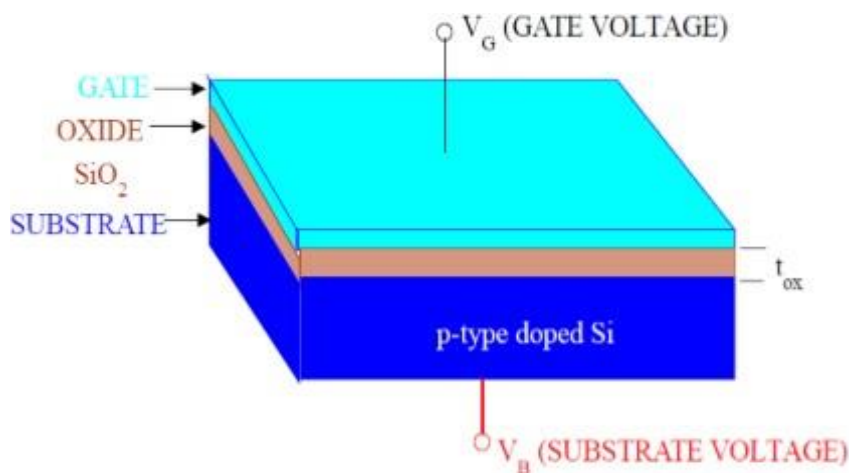


Fig 1.2: MOS STRUCTURE

A MOS capacitor with two p-n junctions situated close to the channel region makes up a MOSFET. The gate voltage controls this region. The substrate potential is kept lower than the potentials of the other three terminals in order to make the p-n junction reverse biased.

An inversion layer will form on the surface and an n-type channel will form between the source and drain if the gate voltage is raised over the threshold voltage ($V_{GS} > V_{TO}$). According to the V_{DS} value, this n-type channel will transport the drain current. As will be shown below, MOSFETs can operate in several areas depending on the value of V_{DS} .

In the region of the inverted channel, thermal equilibrium exists at $V_{DS} = 0$, and the drain current I_D is 0. A drain current proportionate to the V_{DS} will now begin to flow from source to drain through the channel if a small drain voltage, $V_{DS} > 0$, is supplied. From source to drain, the channel provides a continuous path for current flow. Linear region is the name of this technique of operation. The figure below depicts the cross-sectional view of an n-channel MOSFET that is functioning in the linear area.

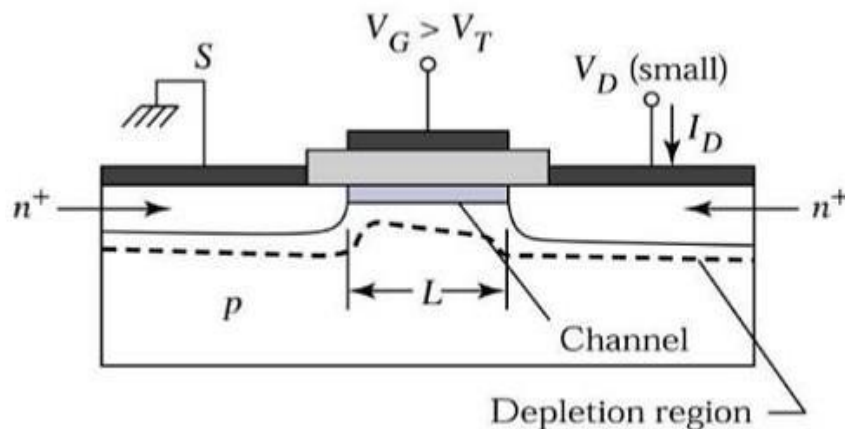


Fig 1.3: Regional Linear

At the Boundary of Saturation, at the end of drain, charges in the channel and channel depth now drop when the V_{DS} is increased. When $V_{DS} = V_{DSAT}$, the channel's charges are reduced to zero, or the pinch-off point. The graphic below depicts the cross sectional view of an n-channel MOSFET that is operating at the edge of the saturation area.

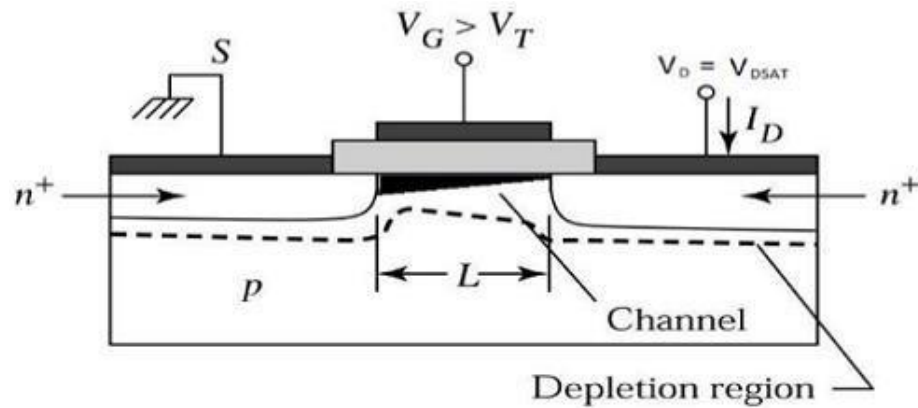


Fig 1.4: Saturation region

1.5 MOSFET BASED SRAM CELL DESIGN PROBLEMS

MOSFET structure scaling into the sub-130 nm regime requires heavy channel doping to control Short Channel Effects (SCE) and heavy super-halo implants to control sub-surface leakage currents. Heavy doping reduces mobility due to impurity scattering and a high transverse electric field in the on state worsens sub-threshold swing and develops parasitic junction capacitance. Therefore, for a given off-state leakage current specification, the on-state drive current is degraded. Off-state leakage current is improved due to band-to-band tunneling between the body and drain. Threshold voltage (V_{th}) variability caused by random dopant fluctuations is another major problem for nanoscale bulk MOSFET devices. With increasing variations, it becomes hard to guarantee near-minimal sized SRAM architecture stability for large arrays in low power embedded applications. Conversely, increasing transistor size is feckless to the fundamental reason for scaling in the first place to increase density. Access time is dependent on the delays and column height. To speed up SRAM cells, segmentation is commonly employed. With further reductions in bit-line height, the overhead area of sense amplifiers becomes essential. In a bulk conventional planar MOSFET based SRAM array, a tremendous increase in leakage current results in large standby power. Moreover, process variations result in contradiction in the strength of different devices in an SRAM cell. Such a contradiction can result in parametric failures, thereby degrading the design yield. Because of the large leakage current and improved parametric variation, designing low-power and robust SRAMs is a major challenge in nanoscale technologies. Due to enhanced short channel effect (SCE), scaling single gate bulk CMOS devices beyond sub-50nm nodes is becoming too hard. Ultrathin body double-gate MOSFET

(DGFET) devices are suitable in sub-50nm technologies due to their higher immunity to short channel effect, better scalability, and increased current compared to single gate devices. Moreover, DGFET has negligible junction capacitance which significantly reduces the circuit delay. Moreover, the body in DGFET devices is lightly doped and the threshold voltage is principally controlled using metal gate work function and this lightly doped body eliminates threshold voltage variations with the help of random dopant fluctuation (RDF).

1.4 PERFORMANCE METRICS OF SRAM CELL

1.4.1 Static Noise Margin (SNM)

The Static Noise Margin is one of the most important metric which is defined as the minimum noise voltage present at each of the cell storage nodes required to flip the state of the cell. SNM is measured by the side of the largest square which is fitted inside the GNRFET based SRAM cross-coupled inverter. This characteristic measured at the time of the read condition ($BL = BL' = VD$, and $WL = VD$). Static Noise Margin is the standard measurement to measure the stability in SRAM architecture cells. The SNM depended on the alternative of the V_{th} for the GNRFET's used in the SRAM cells. A high threshold voltage means that drive current of these type of devices is small which makes the write operation very difficult, thereby, increasing the SNM. One best way to achieve a low power cell along with high stability is to make use of high V_{th} devices. GNRFET devices also provide a high drive current along with a larger V_{th} , thereby, achieving high noise margins along with good write stability.

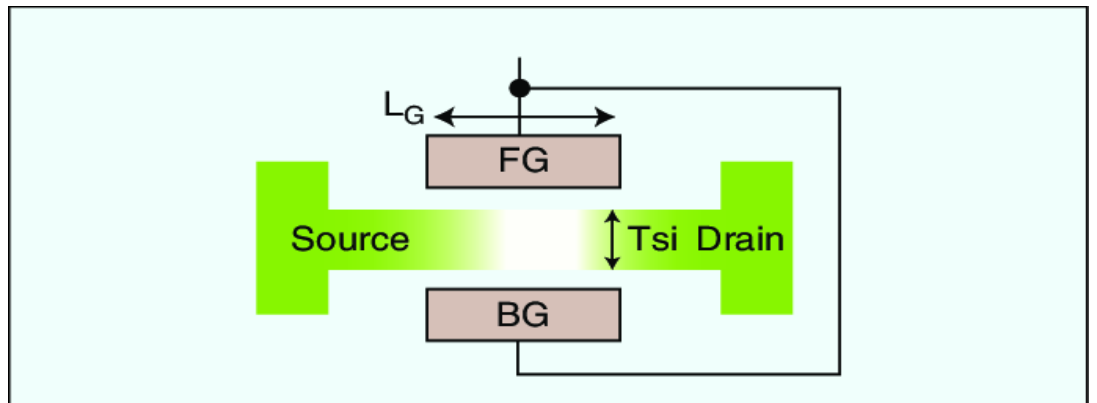


Fig 1.5: Double gate GNRFET

The SNM is seen to be the most responsive to threshold voltage fluctuations in the access and least responsive to the fluctuations in the pull-up pGNRFET device. For GNRFET devices, It is proved that the effect of L_g variation on threshold voltage is small, so the effect on the SNM is also small.

1.4.2 Power and Delay

Power dissipation of the GNRFET SRAM architecture estimate the utility of the cell in movable devices. The primary advantage of the GNRFET based SRAM is its low access time and power dissipation due to low SCE's and leakage current in GNRFET device. While a strong driving current decreases the access time, and increases the power dissipation in the SRAM cell. In SRAM, the propagation delay mainly depends on the column height and delays of the wire. so segmentation is made to decrease the delay. Given that the power-delay-product is always constant for a device, increasing one decreases the other and vice-versa. Enlarging the GNRFET device in SRAM cell decreases the delay at the cost of moderately increased power dissipation. But to reduce power dissipation, leakage currents should be minimized which permit an increase in the channel length or it also leads to higher transistor threshold voltages. Larger channel length results in higher delay and this leads to a trade-off between these two performance indices.

1.4.3 Power-delay-product (PDP)

The power-delay-product (PDP) is defined as the product of the propagation delay and the power consumed of the circuit. It should be minimum for good performance and robustness. Hence we turn to the use of GNRFETs for enhancement of metrics that will make SRAM to perform better.

1.5 CMOS TECHNOLOGY

"Complementary Metal Oxide Semiconductor" is the abbreviation for the word CMOS. The creation of integrated circuits using this technology is widespread today and it is one of the most well-liked technologies in the computer chip design business. This technique is used in today's computer memories, CPUs, and cell phones for a number of reasons. Both P channel and N channel semiconductor devices are used in this technique. The complementary MOS, sometimes known as CMOS, technology is one of the most well-liked MOSFET technologies now on the

market. For microprocessors, microcontroller chips, memory like RAM, ROM, and EEPROM, as well as application-specific integrated circuits (ASICs) technology.

The CMOS Technology uses both NMOS and PMOS to realize various logic functions. Both the N-channel MOSFET and the P-channel MOSFET are design in such a way that they have matching characteristics (during ON and OFF state). The main advantage of CMOS technology over Bipolar or the previous popular NMOS technologies is its extremely low power consumption in static conditions as they draw power only during switching operation. This allows integrating much larger number of logic gates on the VLSI IC when compared to Bipolar or NMOS technologies. Today, CMOS technology is the dominant IC fabrication technology in VLSI industry and is used for making high end microprocessors, microcontroller, memory modules, sensors and Application Specific Integrated Circuits (ASICs). The combination of NMOS and PMOS devices in a CMOS logic makes it easier to design different logic functions. With the improvements in CMOS IC fabrication technologies, the size of the transistor can be scaled down in size. Downscaling the size of the transistor implies that more logical functions can be integrated into the same IC without compromising the speed and power. Initially, the CMOS IC Technology was used in the fabrication of Digital Logic ICs. The development towards low cost and increased functionality has led to CMOS technology being used in Analog ICs and Mixed Signal Designs.

In CMOS technology, logic functions are designed using both N-type and P-type transistors. A transistor of one type is turned OFF using the same signal that turns on the transistor. This property enables the creation of logic circuits without the requirement for a pull-up resistor, using simply straightforward switches.

A group of n-type MOSFETs are positioned in a pull-down network between the output and the low voltage power supply rail (V_{ss} or, more frequently, ground) in CMOS logic gates. CMOS logic gates use a group of p-type MOSFETs in a pull-up network between the output and the higher-voltage rail (often referred to as V_{dd}) in place of the load resistor found in NMOS logic gates.

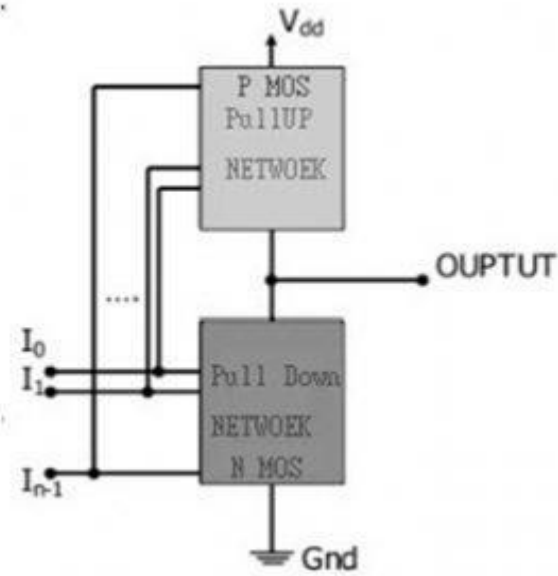


Fig 1.6: CMOS using Pull Up & Pull Down

1.5.1 NMOS Technology

The n-channel MOSFET is called NMOS. It has a substrate of p-type, which consists of majority carrier holes. The n-channel consists of majority carriers electrons. The flow of electrons is fast as compared to holes. Hence, NMOS transistors are more rapid than PMOS transistors. A p-type substrate with diffused n-type sources and drains serves as the foundation for NMOS. Electrons make up the majority of carriers in NMOS. The NMOS will conduct when a high voltage is supplied to the gate. Similar to this, NMOS won't conduct when the gate voltage is low. Since the carriers in NMOS—electrons—travel twice as quickly as the holes in PMOS, NMOS is thought to be quicker than PMOS.

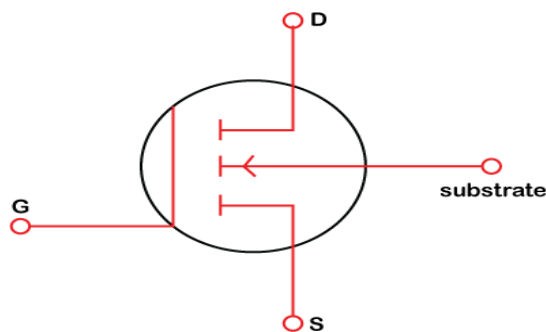


Fig 1.7: NMOS Diagram

1.5.2 PMOS Technology

The p-channel MOSFET is called PMOS. It has a substrate of n-type, which consists of majority carriers electrons. When a negative voltage is applied to the gate end of the PMOS, it repels the electrons. The attraction of holes results in the formation of the channel called the p-channel. The channel is formed between the source and drain. P-type Source and Drain are diffused on an N-type substrate to form a P-channel MOSFET. carriers are primarily holes. The PMOS will not conduct if a high voltage is applied to the gate. The PMOS will conduct when a low voltage is applied to the gate. Compared to NMOS devices, PMOS devices are more noise-resistant.

The slow flow of holes makes the current controlled process of PMOS easy as compared to NMOS transistors.

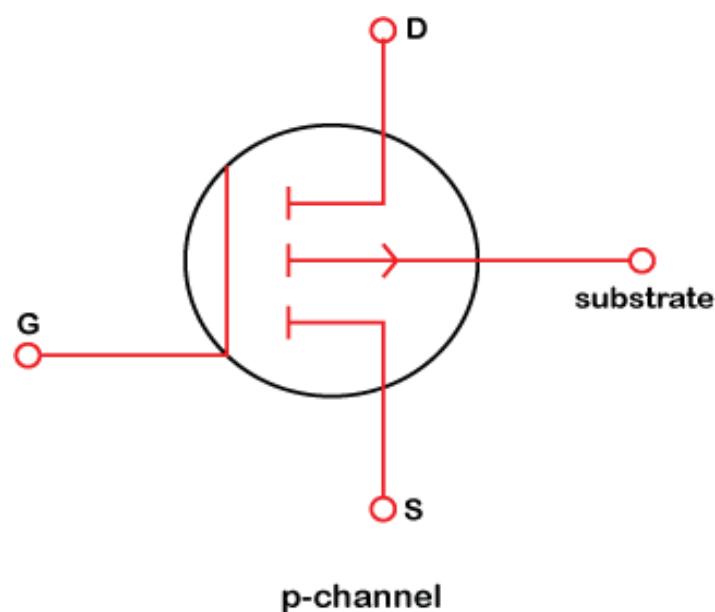


Fig 1.8: PMOS Diagram

1.6 PUF TECHNOLOGY

A PUF can be any physical object that produces these instance-specific measurements. However, in this article we will focus on the best-known subset of PUFs, which are *silicon* PUFs. As the name suggests this specific type of PUF gets its instance-specific measurements from silicon, which means these PUFs are part of an integrated circuit (IC). Due to deep submicron manufacturing process variations, every transistor in an IC has slightly different physical properties. These variations lead to small but measurable differences in terms of electronic properties, such as transistor threshold voltages and gain factor. Since these process variations are not fully controllable during manufacturing, these physical device properties cannot be copied or cloned.

By utilizing these inherent variations, PUFs have been found to be very valuable for use as a unique identifier for any given IC. They do this through circuitry within the IC that converts the tiny variations into a digital pattern of 0's and 1's, which is unique for that specific chip and is repeatable over time. This pattern is a "silicon fingerprint," which is comparable to its human biometric counterpart. Using certain algorithms, which will be described later in this article, the silicon fingerprint is turned into a cryptographic key that is unique for that individual chip and is used as its root key. This root key is reliably reconstructed from the PUF whenever it is needed by the system, without a need for storing the key in any form of memory. So when the device is powered off, no secret key is present in any form of memory; in effect, the root key is "invisible" to attackers, which makes storage of keys with PUFs very secure. Usage of this technology varies from Physical Unclonable Functions for IoT security, where the technology's low cost and flexible implementation offer great benefits, all the way to Physical Unclonable Functions for Aerospace & Defense, proving that the technology is capable of delivering the highest level of security.

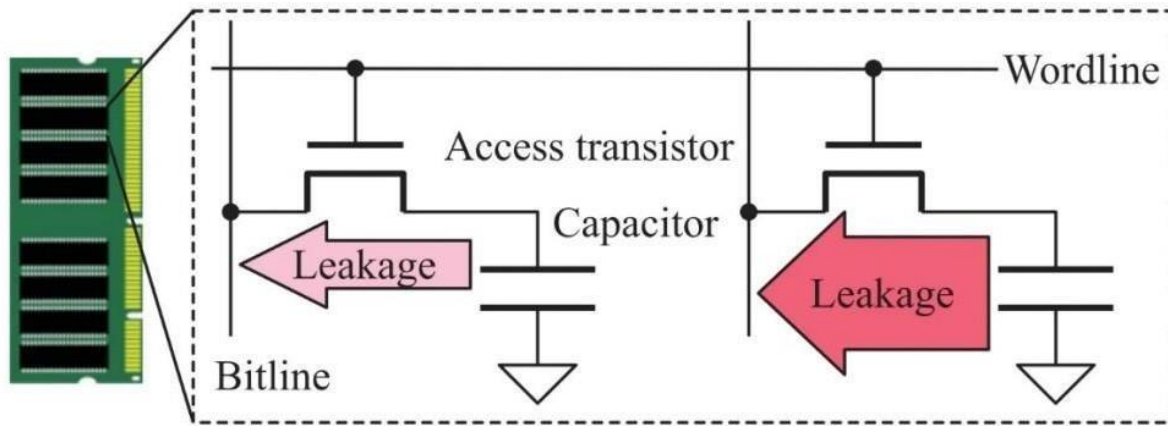


Fig 1.9: PUF Technology

In cryptography and within embedded security ICs, the PUF is used to create keys that are generated on-demand and instantaneously erased once used. PUF is dependent on random physical factors (unpredictable and uncontrollable) that exist natively and/or are incidentally introduced during a manufacturing process. That's why it is virtually impossible to duplicate or clone. PUF technology natively generates a digital fingerprint for its associated security IC, which can be utilized as a unique key/secret to support cryptographic algorithms and services including encryption/decryption, authentication, and digital signature. Except for the momentary duration of a cryptographic operation, the PUF key value never exists in digital form within the circuitry of the security IC. Further, since the key is derived and produced on-demand from physical characteristics of circuit elements, they are never present in the device's non-volatile memory. Any attempt to discover the PUF key through micro-probing or other invasive techniques will disrupt the sensitive circuitry used to construct the PUF key and render the output useless. Thus, they provide a level of security that is very desirable in today's embedded systems.

Each device in Figure 1 has 64 different PUF blocks that generate 1 bit of data. The bits are then shifted to create the 64-bit key. Now our target is to have independent keys for each of these devices that are repeatable over voltage, temperature, and age. Device 1 will produce a key that will have sufficient number of bits that are different from the key produced by Device 2. Each of the device keys, however, will stay constant over the specified voltage and temperature range.

CHAPTER 2

LITERATURE SURVEY

This chapter discusses about the response instability detector that improves bit error rate (BER) performance by discarding unstable response.

2.1 LITERATURE SURVEY

Seungbum Baek et.al., (2021) demonstrated a reconfigurable SRAM-based physically unclonable function (PUF) architecture with numerous challenge-response repairs (CRPs). It adds extra pull-up and pull-down pathways to each SRAM cell when the proposed PUF topology provides a very large CRP area. By eliminating unstable responses, a recently suggested response instability detector enhances bit error rate (BER) performance. A Galois linear feedback shift register is used in the proposed PUF to jumble up the responses, which adds indirect problems (LFSR). In addition to the compact space and quick operating speed that are benefits of the traditional SRAM structure, it may be used in a larger variety of applications as a CRP PUF. A 32X32-bit reconfigurable SRAM was used to test the proposed architecture& performance. A 65 nm CMOS technology is used to construct a PUF array with a 32-bit challenge. By applying an unstable bit discard (UBD) scheme, BER is improved from 13.7% to 0.9%. A unstable bit discard (UBD) strategy is used to reduce the BER from 13.7% to 0.9%.The suggested PUF is demonstrated to be extremely competitive in terms of area, throughput, and energy efficiency when compared to the state-of-the-art. This paper presents a reconfigurable SRAM-based PUF with 160M CRPs. The proposed architecture is the initial one to incorporate cascading pull-up and pull-down signals to produce many CRPs per cell each SRAM; transistors into cross-coupled inverters cell. It is demonstrated that the proposed response instability detector removing unstable responses will help BER performance. In addition to that, the output scrambler adds unrelated difficulties by using a Galois- LFSR, to scramble the response. The proposed PUF was evaluated using a 65 nm CMOS technology. It examines the performance of uniqueness, randomness, and stability under various supply voltages and temperature. To the best knowledge, this is the initial experimental showing the achievement of numerous CRPs within a single SRAM cell. Hence concluding the proposed topology which combines the advantages of weak and

strong memory-based PUFs, can be used as a practical information security system for a highly robust and unpredictable bi-directional authentication.

T. McGrath et.al., (2019) demonstrated the security of the Internet of Things (IoT) in general, and authentication in particular, has emerged as a significant research challenge because security has historically been an afterthought of innovation. Despite the fact that numerous authentication techniques have been put forth in the literature over the past ten years, the majority of them fall short of IoT security and performance standards. Additionally, only a very limited number of these protocols are applicable to Thing-to-Thing (T2T) topologies, in which Things automatically authenticate one another without the need for human involvement. In this research, we propose the T2T-MAP, a novel lightweight PUF-based T2T mutual authentication mechanism (Physical Unclonable Functions). By utilising the physical unpredictability of each Thing's circuitry, the protocol uses PUFs technology to enable each Thing to individually identify and authenticate itself in an IoT infrastructure. To demonstrate that the protocol is secure against known attacks, we develop it and do a security study. Additionally, we use a security protocol prover to demonstrate the protocol's security. In order to show that the protocol enables quick authentication, manageable communication overhead, and low energy consumption, we finally develop a prototype of the protocol on devices with limited resources and then undertake a performance analysis.

J. R. D. Kumar et.al., (2021) demonstrated the field of IC technology grows every day and it plays a decisive role in a day to day activity. One of the most emerging fields is biomedical. This field is getting with er and the size of the devices becomes reduced from ECG machines to portable medical devices. Nowadays wearable devices and implantable biomedical devices on the body captures the biosignals and convert it as potential signals to measure the variation and the devices which are connected to the cloud using IoT technology is helpful to digest the types of problem with less time and better accuracy.

M. Bhargava et.al., (2010) demonstrated various security applications use Physically Unclonable Functions (PUFs), which provide die-specific random functions. A major worry is the stability or dependability of a PUF response, particularly when the IC housing the PUF is subjected to extreme environmental fluctuations. Errors in response bits must be completely repaired in cryptographic

applications, and this is frequently accomplished via pricey error correction algorithms (ECC). However, complete answer bit correction is not required in applications for identity and authentication, therefore pricey ECC techniques can be avoided. On the other hand, one-way functions cannot postcondition a response with broken bits, making it more susceptible to modelling attacks. We suggest a PUF (SA-PUF) structure based on sensing amplifiers that produces random bits with higher dependability and much fewer response bit mistakes. As a result, there is no longer a need for elaborate and expensive ECC hardware in cryptographic applications. The employment of one-way functions to post-condition the outputs even in identity and authentication applications becomes more viable with the lower implementation cost of ECC, hence boosting their resistance to modeling-based attacks. Finally, compared to the majority of the earlier proposed silicon based PUF designs, SA-PUF elements are naturally more resistant to environmental changes. As a final point, SA-PUF elements are naturally more resistant to environmental changes than the majority of the earlier proposed silicon based PUF designs.

K.-U. Choi, et.al., (2020) demonstrated a physically unclonable function (PUF) with individually embedded non-volatile memory (eNVM) that provides 100% stable random bits is discussed in this study. The suggested eNVM biases the sense-amplifier to always replicate the same key as the initial value through a feedback loop, where it saves the initially generated random key. A 256-bit PUF with a core area of 0.160 mm² was constructed in a 180 nm standard CMOS process to test the performance of the suggested architecture. The measured Hamming Distances (HD) for the implemented PUF are 0 within the chip (100 percent stability) and 0.5047 between the chips.

M. Hiller et.al., (2016) demonstrated Silicon Physical Unclonable Functions (PUFs) produce a sequence of response bits from chip-unique manufacturing variations Using error correction methods, bit-exact cryptographic keys are created. To simplify implementation, the error correction is often divided into separate processing blocks. The consistency of PUF responses vary from bit to bit, but there hasn't been much research done to mathematically assess how the consistency of PUF response sequences is affected by block size. We demonstrate that the likelihood of drawing an unreliable sequence declines exponentially with block size using the typicality idea from information theory. We introduce Differential Sequence

Coding (DSC), which scales effectively for higher block sizes without the super-linear increase in decoding complexity of earlier methods. It sequentially examines the full PUF answer before only doing the cryptographic key generation on a single, very reliable block. Our example of a convolutional code implementation in an FPGA is made for a typical SRAM PUF application. It only uses 974 PUF bits and 1,108 auxiliary data bits to construct a 128 bit key with an output bit error probability of 6.14109 and an average input bit error probability of 15%. Without significantly increasing the implementation size of the key generation module, there are 36% fewer PUF bits and 71% less helper data bits than the best previous individual outcomes in both categories.

M. T. Rahman et.al., (2017) demonstrates a reconfigurable SRAM-based physically unclonable function (PUF) topology with several challenge-response pairs (CRPs) per cell is shown in this study. By adding additional pull-up and pull-down paths to each SRAM cell, the proposed PUF topology provides a very large CRP area. The challenge inputs activate these alternative routes to the supply rail and ground, essentially reconfiguring each cross-coupled inverter's transfer characteristics. By eliminating unstable responses, a recently proposed response instability detector enhances bit error rate (BER) performance. A Galois linear feedback shift register is used in the proposed PUF to jumble up the responses, which adds indirect problems (LFSR). Because the suggested PUF contains numerous CRPs in addition to the small space and quick operating speed that are advantages of the traditional SRAM structure, it may be used in a larger variety of applications as a CRP PUF. A 3232-bit reconfigurable SRAM PUF array with a 32-bit challenge is developed in a 65 nm CMOS process to test the performance of the suggested architecture. The inter-chip Hamming distance (HD) over 40 chips is 48.93%, the core area is 88.867 m²/bit, and the energy efficiency is 0.082 pJ/bit, according to experimental data. A unstable bit discard (UBD) strategy is used to reduce the BER from 13.7% to 0.9%. The suggested PUF is demonstrated to be extremely competitive in terms of area, throughput, and energy efficiency when compared to the state-of-the-art.

L. Lin et.al., demonstrated that there has been a lot of research on how to improve hardware security and IP protection by utilising the special physical features

of integrated circuits. Physically unclonable functions (PUFs) can identify chips by detecting natural manufacturing variations. We examine the effects of process technology and supply voltage scaling on arbiter-based PUF circuit design to enable the integration of PUFs into low-power and security applications. Advanced technologies and lower supply voltage can enhance the PUF uniqueness due to greater delay sensitivity, according to a Monte Carlo-based statistical analysis. By accounting for fluctuations in the device, supply voltage, and temperature, a PUF delay profile has been generated using a linear regression method. The PUF additive delay behaviour is confirmed using a precise SVM-based software modelling analysis. Finally, the discrepancy between simulation findings and postsilicon validation results on arbiter-based PUF test chips in 45 nm SOICMOS technology has been discussed. Due to the limitations of our delay model and the impacts of dynamic circuitry, the test chips can withstand the basic SVM attack.

C.-C. Chang.et.al., (2011) demonstrated SVM for classification, regression, and other learning tasks, Support Vector Machines (SVMs) are a well-liked machine learning technique. We have been creating the package LIBSVM as a support vector machine library from the year 2000. However, the goal of this paper is not to impart knowledge about LIBSVM's actual application.

Kan Xiao.et.al.,(2014) demonstrates Environmental changes and ageing have an impact on Physically Unclonable Functions (PUFs), which can lower their adoption in identifying and authentication applications. Bit analysis across environmental conditions, better design, and post-processing error correction are a few previous methods to increase PUF reliability, but they come at a high cost in terms of test time and design overheads, making them unsuitable for big scale manufacture. In this research, we propose unique bit analysis and bit selection techniques to solve this problem for SRAM PUFs. Our analysis of actual SRAM PUFs reveals I critical factors to consider when choosing stable SRAM cells for PUF at a low cost (ii) previously unresearched spatial correlation between stable bits, i.e., cells that are the most stable tend to be surrounded by stable cells determined during enrolment. Based on these facts, we create a bit selection process that yields

extremely stable bits for the ID/key generated by the PUF. Our approaches can effectively reduce the number of errors in PUF IDs/keys with fewer enrollment stages, according to experimental data from actual SRAM PUFs.

Jiliang Zhang et.al., (2021), Strong bodily unclonable function (PUF) is a promising answer for tool authentication in resource constrained programs however liable to system studying assaults. In order to withstand such attack, many defenses have been proposed in current years. However, those defenses incur excessive hardware overhead, degenerate reliability and are inefficient towards superior system studying assaults which includes approximation assaults. In order to cope with those issues, we suggest a Random Set-primarily based totally Obfuscation (RSO) for Strong PUFs to withstand system studying assaults. The fundamental concept is that numerous stable responses are derived from the PUF itself and pre-saved as the set for obfuscation withinside the trying out phase, after which a true random range generator is used to choose any keys to obfuscate demanding situations and responses with XOR operations. When the range of challenge-reaction pairs (CRPs) accrued via way of means of the attacker exceeds the given threshold, the set could be updated immediately. In this way, system studying assaults can be averted with extraordinarily low hardware overhead. Experimental consequences display that for a sixty-four×sixty-four Arbiter PUF, while the scale of set is 32 or even if 1 million CRPs are accrued via way of means of attackers, the prediction accuracies of Logistic regression, aid vector machines, synthetic neural network, convolutional neural network and covariance matrix adaptive evolutionary approach are about 50% that's equal to the random guessing.

G. T. Becker et.al., (2015), demonstrate the primary real-world biological research attack on an advert PUF-based RFID tag. The examined commercial PUFs will be attacked by activity solely four protocol executions, that takes under two hundred ms. employing a RFID smartcard emulator, it then doable to impersonate, i.e., “clone” the PUF. whereas offensive the 4-way PUF employed by these tags will be done mistreatment ancient machine learning attacks, we have a tendency to show that the tags can still be attacked if they organized as presumptively secure

XOR PUFs. we have a tendency to achieved this by using a new reliability-based machine learning attack that uses a divide-and-conquer approach for offensive the XOR PUFs. This new divide-and-conquer approach ends up in solely a linear increase in required range of challenge associated responses for increasing numbers of XORs. this can be in stark distinction to the progressive machine learning attacks on XOR PUFs that are shown to possess an exponential increase in challenge and responses.

Abhranil Maiti et.al., (2010), To validate the effectiveness of a Physical Unclonable Function (PUF), it wishes to be characterised over a big populace of chips. Though simulation strategies can provide approximate consequences, an on-chip test produces more correct result. In this paper, we symbolize a PUF primarily based totally on ring oscillator (RO) the usage of a appreciably big populace of 125 FPGAs. We examine the experimental facts the usage of a hoop oscillator loop put off model, and quantify the first-rate elements of a PUF such as area of expertise and reliability. The RO-PUF indicates a mean inter-die Hamming distance of 47.31%, and a mean intra-die Hamming distance of 0.86% at ordinary running condition. Additionally, we want to make this big RO frequency dataset to be had publicly for the studies community.

B.Karpinskyy et.al.,(2016), Physically unclonable function (PUF) circuits are for producing particular steady keys or chip IDs primarily based totally on intrinsic houses of every chip itself [1-2]. PUFs are a leap forward to enhance the safety stage as compared to conventional NVM (non-unstable memory) solutions (FUSEs, EEPROM/FLASH, etc.) due to the fact they solve protection issues, including energetic records- probing, shifting the safety key from outside, etc. Since the MOSFET mismatch (e.g. size, doping concentration, mobility and oxide thickness) because of procedure versions cannot be completely controlled, PUFs, which can be primarily based totally on such phenomena, cannot be replicated. Unfortunately, the PUF output is faulty with the aid of using nature, as resulting from thermal noise, voltage/temperature influence, ageing effects, etc. The balance difficulty ought to be triumph over on the grounds that general protection applications, including records

encryption and virtual signatures, have 0 mistakes- tolerance. In this work, a PUF shape primarily based totally on the edge voltage (V_{th}) distinction of inverting common sense gates is presented, that's applied for steady 24b key era in a 45nm clever card chip. The secret is used as a part of an encryption key and achieves an mistakes fee as little as 2.01×10^{-38} . The PUF machine is likewise scalable for a bigger key size.

Armin Babaei, et.al., (2019) Attacks on Internet of Things (IoT) devices are increasing. Physical Unclonable Functions (PUFs) are proposed as a robust and lightweight solution to protect IoT devices. The main advantage One PUF compared to today classic crypto solutions is its compatibility with IoT devices with limited computing resources. In this white paper, we examine the maturity of this technology and the challenges of using PUFs in the IoT that still need to be addressed.

S. Kumar V, et.al.,(2006) describes the assessment and evaluation of SRAM cells offers important statistics for buying and selling of layout parameters to satisfy stringent necessities withinside the deep sub-micron ranges. Initially this paper introduces to SRAM cells, then mobileular parametric dependences are investigated and ultimately simulation outcomes of the equal are shown. An 11T SRAM mobileular is in comparison with the traditional 6T SRAM mobileular for SNM, Power, DRV and Bit Line capacitances versions. The effect of those parameters versions is investigated in element and simulations outcomes of the equal is discussed.

Yansong Gao, et.al.,(2020) a Physical Unclonable Function (PUF), is a device that exploits the inherent randomness introduced during manufacturing to give a physical entity a unique 'fingerprint' or trust anchor. These devices can be used in a variety of applications from anti-counterfeiting, identification, authentication and key generation to advanced protocols such as forgotten transmission, key exchange, key renewal and virtual reality testing. Here we discuss the development of PUFs, including those that take advantage of optical functions, circuit time delays, and volatile/non-volatile memory functions. We examine the various PUF applications and consider the security issues they face, pointing out known attacks and possible

countermeasures. We also consider Key areas for future developments such as bit-specific reliability, reconfigurability and public key infrastructure.

Ding Deng, et.al.,(2008) Physical unclonable function (PUF), a hardware that may extract the variations of the same implementations and offer specific mystery keys without the usage of non-risky memory, is regarded as a promising safety primitive withinside the close to future. Ring Oscillator (RO) PUF is certainly considered one among its smooth silicon implementations, which exploits the frequency distinction among a couple of structurally equal ring oscillators. However, a big quantity of ROs need to be built if a couple of strong output bits are required, this means that unacceptable region overhead for light-weight applications. To remedy this problem, configurable ROs the use of multiplexers and special postpone devices had been proposed in preceding papers. Unfortunately, most of them take gain of the precise shape of a positive sort of field-programmable gate arrays (FPGAs), accordingly now no longer cost-saving for application-precise included circuit (ASIC).

Masoud Rostami, et.al., (2014) The multinational, distributed, and multistep nature of incorporated circuit (IC) manufacturing deliver chain has added hardware-primarily based totally vulnerabilities. Existing literature in hardware safety assumes advert hoc chance models, defences, and metrics for evaluation, making it hard to research and examine change solutions. This paper systematizes the current understanding on this rising field, which includes a category of chance models, present day defences, and evaluation metrics for vital hardware-primarily based totally attacks.

Yuan Cao et.al., (2019) depicts the burgeoning hardware security primitive for physical non-clonable functions (PUF) has sparked interest from the solid-state circuit community in its efficient integration into security-critical applications. This paper presents an energy efficient implementation of the classic referee PUF design. Current hungry (CS) inverters are inserted at the inputs of each multiplexer cell to reduce bias and widen distribution the delay difference between two series-connected symmetrical delay paths, which can be selected by the input query. CS inverters are biased at the zero temperature

coefficient (ZTC) point, which makes the cumulative delays of the two identical paths insensitive to temperature variations. A symmetric arbiter based on two RS latches is proposed to overcome the asymmetric input and clock-to-output propagation delay of the D flip-flop and the metastability problem of the RS latch arbiter.

2.2 LITERATURE SUMMARY

To implement the response instability detector that improves bit error rate (BER) performance by discarding unstable response, the proposed architecture integrates multiple CRPs into each SRAM cell for the first time by cascading pull-up and pulldown transistors into cross-coupled inverters. The uniqueness, randomness, and stability of the proposed PUF were measured at various voltage levels and temperatures. It is implemented in a 65 nm CMOS process. The proposed architecture can be used as a real information security system for a highly reliable and unpredictable bi-directional authentication since it combines the benefits of weak and strong memory-based PUFs.

2.3 PROBLEM DEFINITION

To analyze the Performance Analysis of an Efficient VLSI Architecture using GNRFET Technology.

CHAPTER 3

EXISTING METHODOLOGY

In this we discuss about Reconfigurable SRAM PUF with Challenge Response Pairs

3.1 OPERATING PRINCIPLE OF RECONFIGURABLE SRAM PUF

In a typical SRAM PUF, the structure of a unit cell and the voltage transfer characteristics under both ideal and real-world circumstances are shown in Fig. 3.1. The unit cell of the SRAM PUF is represented in Fig.3.1(a) as a cross-coupled pair of inverters with complementary outputs (V_{OUT} and $V_{OUT B}$) that depend on physical mismatch brought on by process variation. The intersection of the x- and y-axes, denoted by the dashed line in Fig.3.1, represents the location of the metastable point under idealized circumstances in which both inverters are precisely similar and there is no noise (b). In actuality, the scenario will resemble Fig.3.1(c) and(d). Cross-coupled inverters' pull-up and pull-down networks drive the outputs to VDD. Due to a little offset brought on by process mismatch, the pull-up and pull- down networks of cross-coupled inverters drive the outputs to VDD and ground, respectively. Due to unpredictable process variation, the output values are random and physically unclonable even if the SRAM architecture in Fig.3.1 (a) is duplicated. The typical SRAM cell can respond even when there is no challenge input. The SRAM PUF cell's response will settle more quickly and become more resistant to noise and other environmental variation as soon as the metastable point starts to diverge from the intersection boundary during initialization. This helps in ID generation. On the other hand, when there is a slight mismatch, the circuit's stochastic noise generates the response at random.

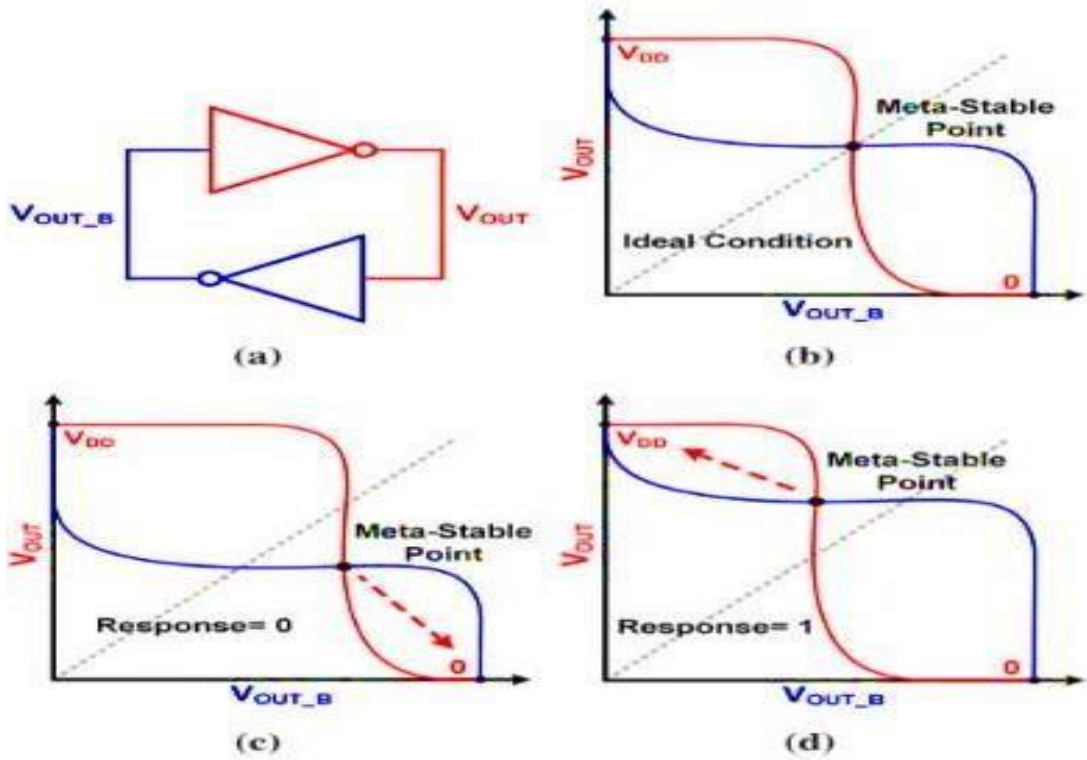


Fig 3.1: Basic Structure of Conventional SRAM PUF

Fig. 3.2 depicts a schematic of the suggested reconfigurable SRAM PUF with several CRPs. It comprises of many cross-coupled inverters with challenge inputs applied to cascade pull-up and pull-down transistors (see Figs.3.2(a) and 2(b)). The point of metastability can be randomly shifted by altering the multi-bit challenge by changing the relative strength of the pull-up network (PUN) and pull-down network (PDN) (Fig.3.2(c)). Through the use of many CRPs enabled from a single SRAM PUF unit, this method transforms the weak PUF into a CRP PUF. There must be matching cross-coupled inverters of the same strength on each side of the inverters in Fig.3.2(c). By doing this, it is ensured that physical mismatch, rather than a deterministically delivered voltage, is what causes the reaction. The gate terminals of the cascade transistors are linked to the challenge input. The linkages between the challenge inputs and SRAM PUFs have little impact on the PUF replies because the gate impedance is theoretically limitless.

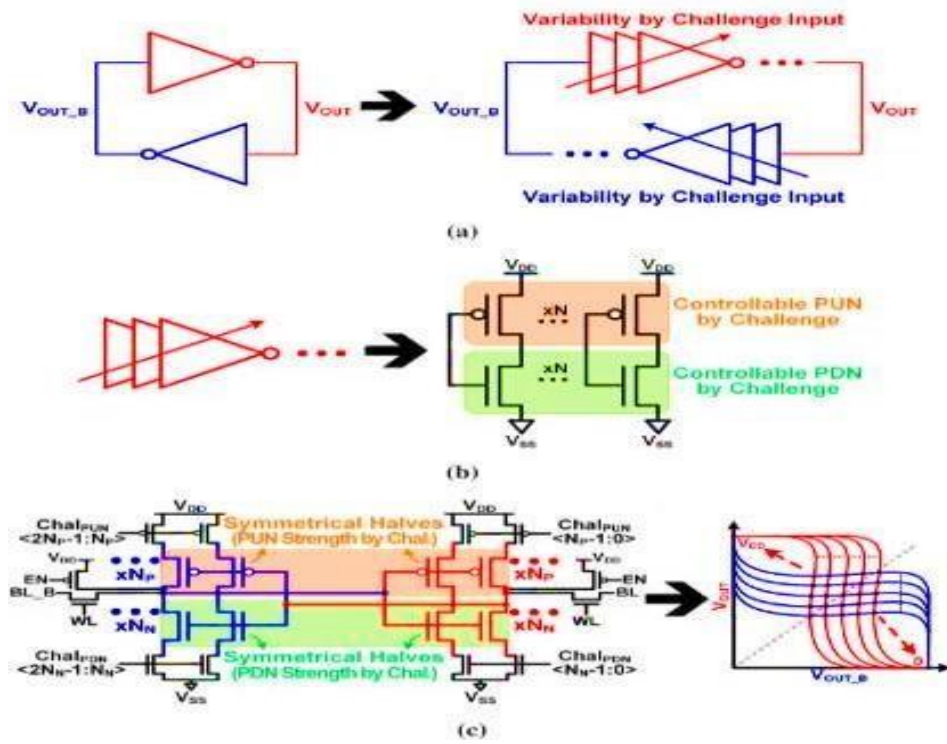


Fig 3.2: Conceptual Structure of Reconfigurable SRAM PUF Unit.

Fig. 3.3 depicts a straightforward example where, for a given challenge input, the number of NMOS and PMOS equals $N_N = N_P = 2$. As a result of process variation, the challenge from C0 to C7 changes the SRAM cell characteristics, producing new mismatch combinations. The PDN/PUN strength is affected cumulatively by the process variation of each inverter, allowing for a quicker transition to a stable state. If only one PMOS transistor with C0 = 0 and C1 = 1 is switched on in Fig.3.3 (b), there are two possible configurations in the cell: C2 = 1 and C3 = 0 or C2 = 0 and C3 = 1, which is the same number of transistors that must be turned on to have the same strength for both configurations. The suggested PUF accepts two combinations of challenges for C0 = 1 and C1 = 0, respectively. There is just one situation in which all PMOS transistors are on, and that is when both transistors are on. As a result, there are 5 possible responses to the PMOS transistor issues with $N_P = 2$ in the suggested reconfigurable SRAM PUF. Ultimately, the proposed SRAM PUF yields 25 (55) CRPs, which are the sum of the NMOS and PMOS possibilities, for an 8-bit challenge input ($N_N = N_P = 2$). NMOS and PMOS possibilities, for an 8-bit challenge input ($N_N = N_P = 2$).

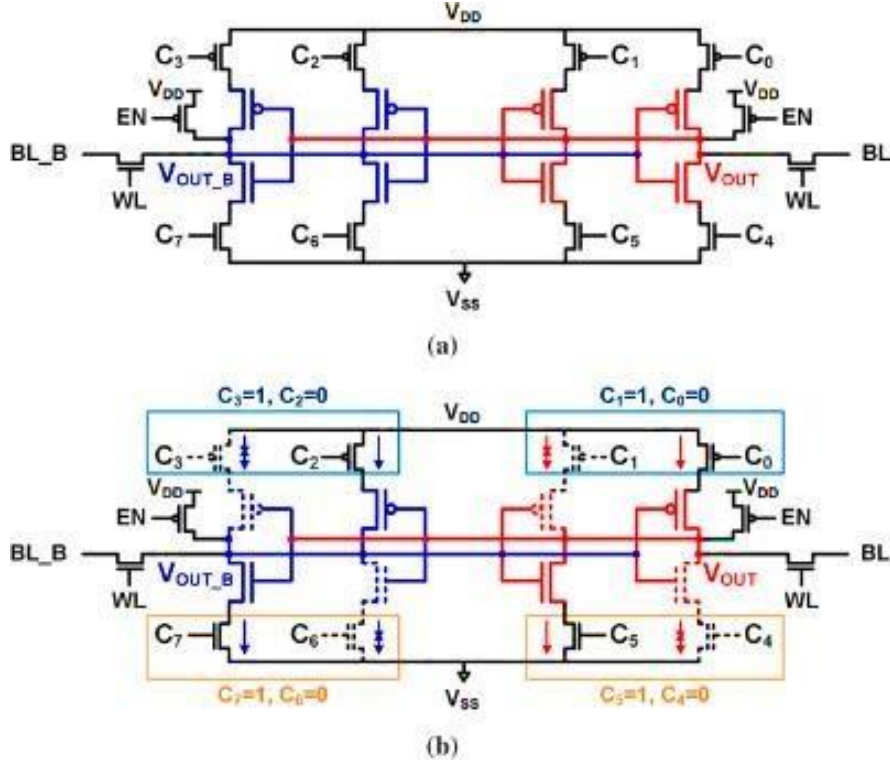


Fig 3.3: Schematic of Reconfigurable SRAM

3.2 IMPLEMENTATION OF OVERALL RECONFIGURABLE SRAM PUF SYSTEM

The proposed PUF chip's system architecture and timing diagram are shown in Fig. 3.4, where the reconfigurable In Fig.3.2, an SRAM PUF cell with 32-bit challenges and $NN = NP = 8$ is shown (c). The PUF chip is made up of a 1024-bit (3232) array with a response instability detector, a scrambler that can optionally permute the response to increase complexity, and a controller to switch between different permutations of the response. Reset, assessment, and scramble are the three operational modes. All blocks are initialized by synchronously resetting to create CRPs. During reset mode, all signals—aside from the challenge—input to either "1" or "0." The array evaluation stage that follows produces 32-bit output using the inputs from the challenge. According to Fig. 4, a single CRP generation requires at least two clock cycles for PUF reset and evaluation (b). A serial to parallel interface circuit can produce the challenge using an external input signal. The alternative method of creating challenge input is to use random bitstream input that satisfies the challenge constraint.

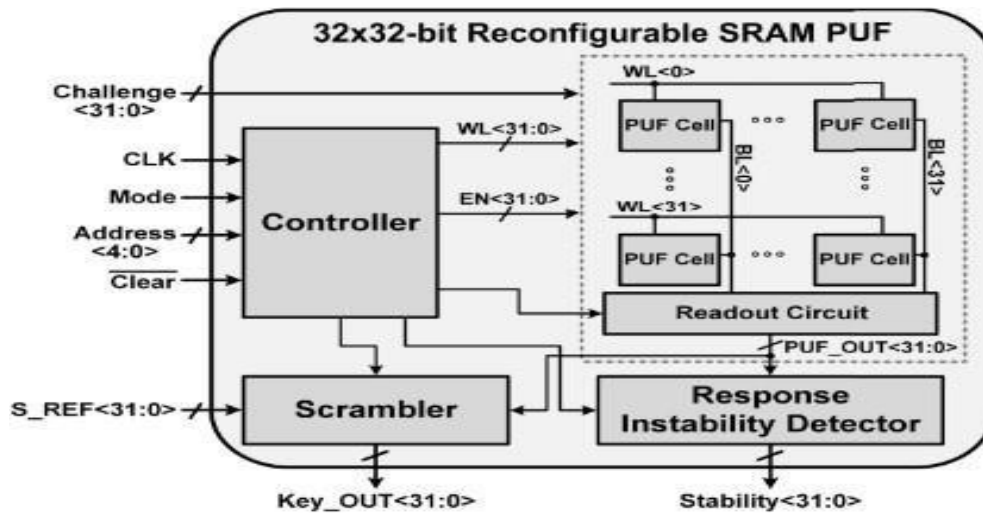


Fig 3.4 Architecture and Waveform of SRAM PUF Chip

A shift register and a binary counter could be a part of the circuit. Once a random bitstream has been created using a PRNG, the counter compares the challenge strengths of each side, and for a challenge section with a lower strength, a new random bit from the PRNG is injected using a shift register. The preset challenge is passed to the PUF circuit once the circuit determines that both sides of the challenge are of equal power. A response instability detector filters the responses. The same chip should ideally reproduce the same response for the same challenge input, however in evaluation mode a random response must be created across distinct chips. Under the same challenges, the response instability detector picks up instances of bit-flipping.

The addresses of cells that are sensitive are sent to the Stability signal because bit-flipped cells have a high likelihood of producing an unstable response to a specific stimulus. During examination, these cellular responses are disregarded. In scramble mode, the scrambler optionally transforms the 32-bit response's input string (PUF OUT) into an output string that has been XORed and of the same length. In the suggested structure, the answer is randomized or bypassed according to the S REF signal by the scrambler implemented with the Galois-configuration LFSR. The quantity of response permutations that must be carried out is likewise determined by the S REF signal. When $NP = NN = 8$ in Fig. 2 (c), the transistor-level

schematic of the implemented SRAM PUF cell unit, which consists of 16 inverters and a 32-bit challenge input, is shown in Fig. 5(a). According to Eq. (5), the total capacity of CRPs is 1.6×10^8 when $N_P = N_N = 8$. Fig. 5 displays the time diagram related to reading the response from the bit line (BL) (b). The cascade transistors serve multiple functions, including initializing the cell during reset as well as sending the challenge signal to the inverters. The cascade transistor is turned off during initialization in order to prevent VDD and VSS from being sent to the output nodes. An active-low signal supplied to EN securely recharges the two output nodes to "1." In a similar way, the bit line can also be pre-charged. The evaluation phase starts after the pre-charge phase is finished by applying the challenge bits, which causes the SRAM unit to reach its metastable point. The output that is sent to BL and BL B through WL will then stabilize due to the cross-coupled inverter network's positive feedback.

In terms of layout technique, parasitic components should be carefully examined to make the left and right side of the PUF core balanced by designing the layout in a symmetric form that includes metal, via, and contact in order to reduce layout effects other than physical changes. Additionally, symmetry must be maintained in the link between SRAM and the transistors that make up the challenge input. While pursuing low systematic components, the suggested SRAM PUF is laid out with the smallest devices possible to accommodate high random changes.

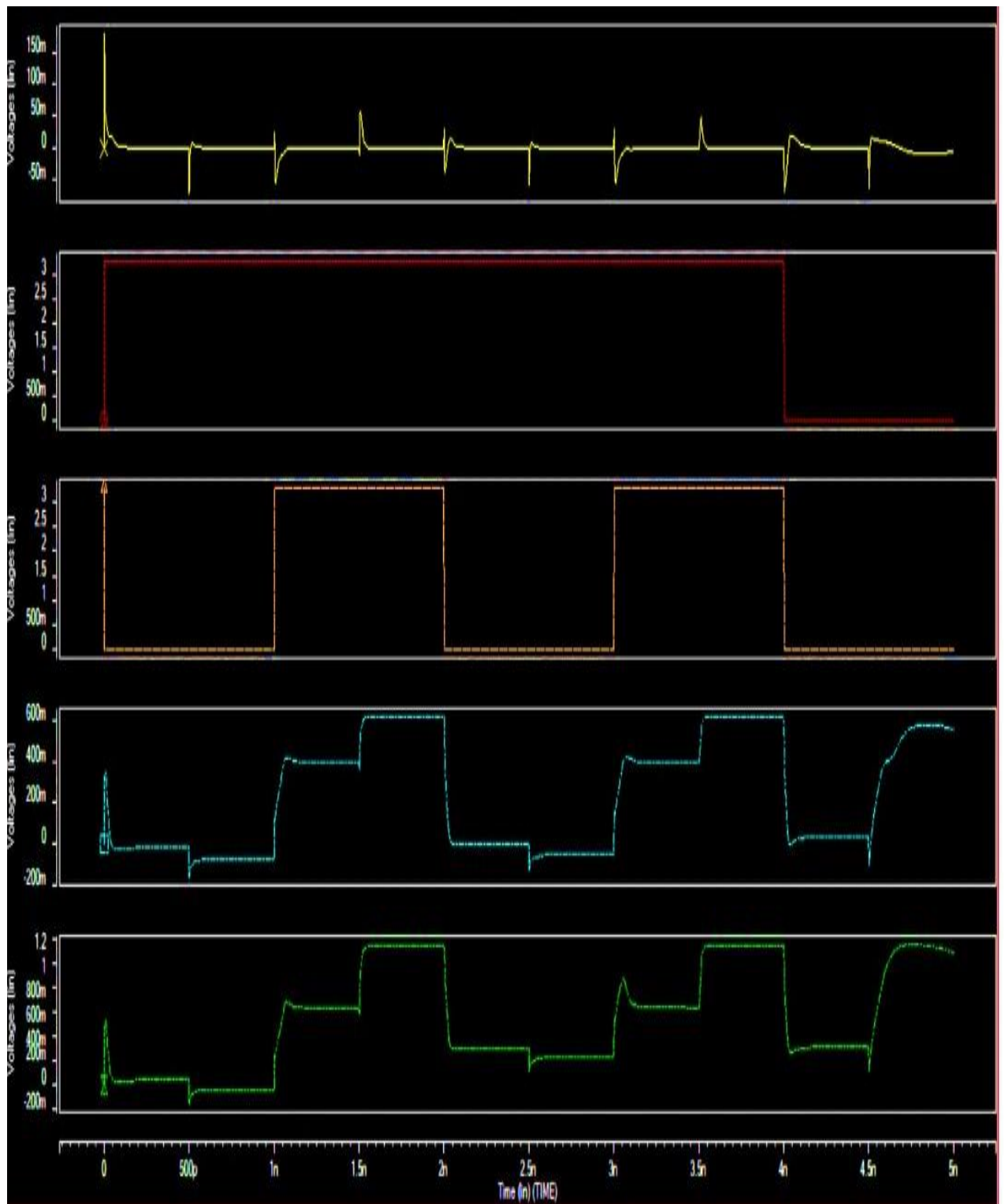


Fig 3.5: Output for Existing Analysis

Table 3.1 Analysis for performance of MOSFET

Device	Power	Delay
ADDER	4.14×10^{-9}	304.11×10^{-12}
AND	5.11×10^{-9}	347.98×10^{-12}
DFF	11.19×10^{-9}	376.26×10^{-12}
Proposed reconfigurable SRAM PUF cell	58.23×10^{-9}	94.11×10^{-12}
MUX	74.21×10^{-9}	347.24×10^{-12}
SRAM	46.11×10^{-9}	47.11×10^{-12}

CHAPTER 4

PROPOSED SYSTEM

In order to improve efficiency, existing system as SRAM PUF architecture will be analyzed using 130nm,32nm CMOS Technology. Further, SRAM PUF architecture will be modified and analyzed using 130nm,32nm CMOS Technology. In terms of power, speed and power delay product. Also, the proposed system will be analyzed and compared 16nm GNR-FET Technology. This outperforms an efficient SRAM PUF architecture for high speed and low power applications.

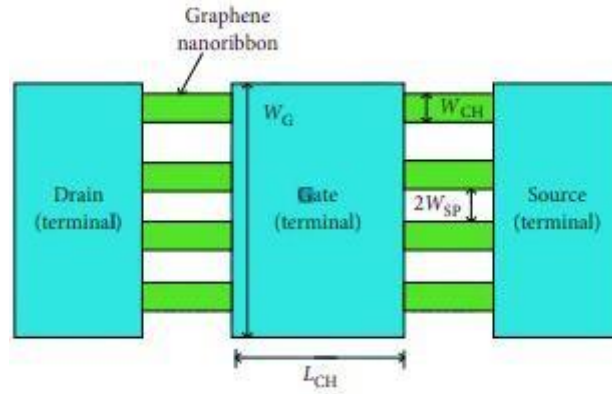


Fig 4.1: The structure of a MOSFET like GNR-FET

Figure 4.1 shows the design of a GNR-FET that resembles a MOSFET and features parallel ribbons connecting from the source, gate, and drain to boost drive strength. The channel can be managed by a +e gate. L_{ch} stands for the channel length, W_{ch} for the ribbon width, and $2W_{SP}$ for the distance between the ribbons. Table 4.1 displays the GNR-FET device parameters used in this study. For MOSFET, GNR-FET, and GNR-FET, Predictive Technology Models (PTMs) and Urbana Champaign Model, respectively, are utilized as SPICE models. Short-channel effects, which are common in sub-100 nm Si MOSFETs, can be mitigated with GNR-FETs.

Device parameters	Values
Length of the channel	15 nm
Top gate dielectric material thickness	0.95 nm
Space between adjacent GNRs	2 nm
No. of GNRs	6
Substrate oxide thickness	20 nm
No. of dimer lines in GNR lattice	12

Table 4.1 Device parameters of graphene nanoribbon field-effect transistor

The performance of GNRFET electrical devices is the main topic of this section. According to theoretical research, the band gaps in GNRs are inversely proportional to their widths. The edge state also affects conductivity in several ways. GNRs with mainly zigzag edges show metallic properties, but GNRs with mainly armchair edges are found to be semiconducting. Commonly, the number of dimer lines N is used to define the width of a GNR (abbreviated W_{ch}), where $WCH = 3d_{cc} (N+1)/2$, where d_{cc} is the carbon-carbon bond distance at 0.142 nm. As a result, the length is 15 nm and the width is 0.86 nm for both the PGNR and NGNR models. Two extra n-type transistors with an additional bit line and control signal are used to separate the cell core from the output. Through the access transistors, the write mode is carried out. The data saved is accessed using the +e access mode, and it is displayed on the access bit. The design's +e cross-coupled inverters are open-circuited for the write mode because the feedback loop is only required for access mode data storage. The I_d - V_d characteristics of GNRFETs at various gate voltages ranging from 0 V to 1 V can be used to assess device performance. The I_d - V_g transfer characteristic of symmetrical n-type and p-type GNRFET for $|V_d| = 0.1$ V and $|V_d| = 1$ V is shown in Figure 4.2.

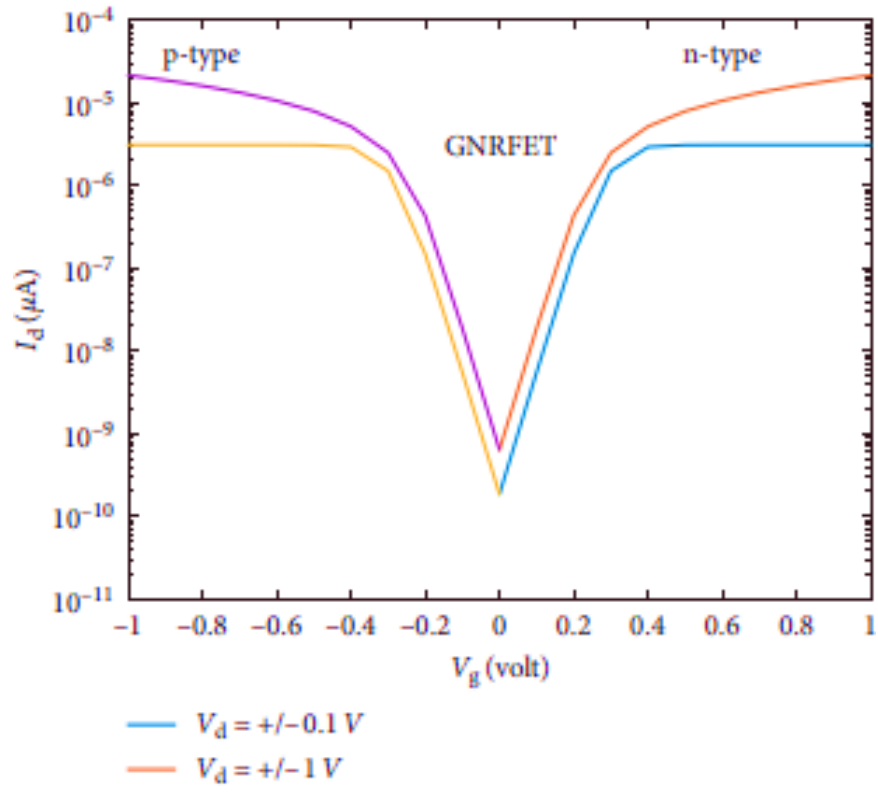


Fig 4.2: I_d - V_d transfer characteristics of symmetrical n-type and p-type GNR-FET for $|V_d|=0.1 \text{ V}$ and $|V_d|=1 \text{ V}$.

4.1 SIMULATION OF WAVEFORMS USING 32NM MOSFET TECHNOLOGY

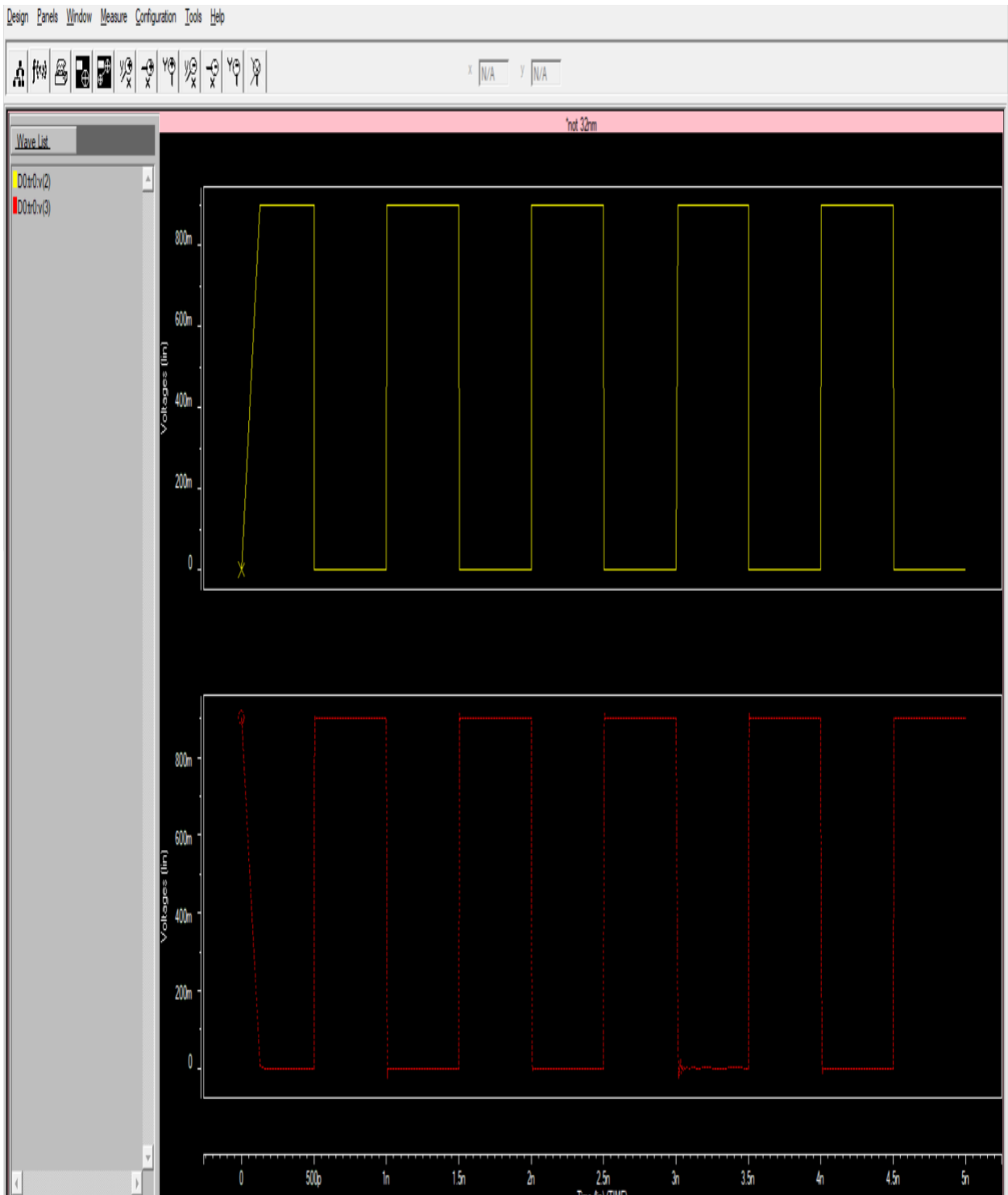


Fig 4.3: Simulation results for NOT gate using 32nm MOSFET Technology

Figure 4.1.1 shows the simulation output of NOT Gate 32nm MOSFET technology. The inputs given were v(2) and the output is taken by v(3).

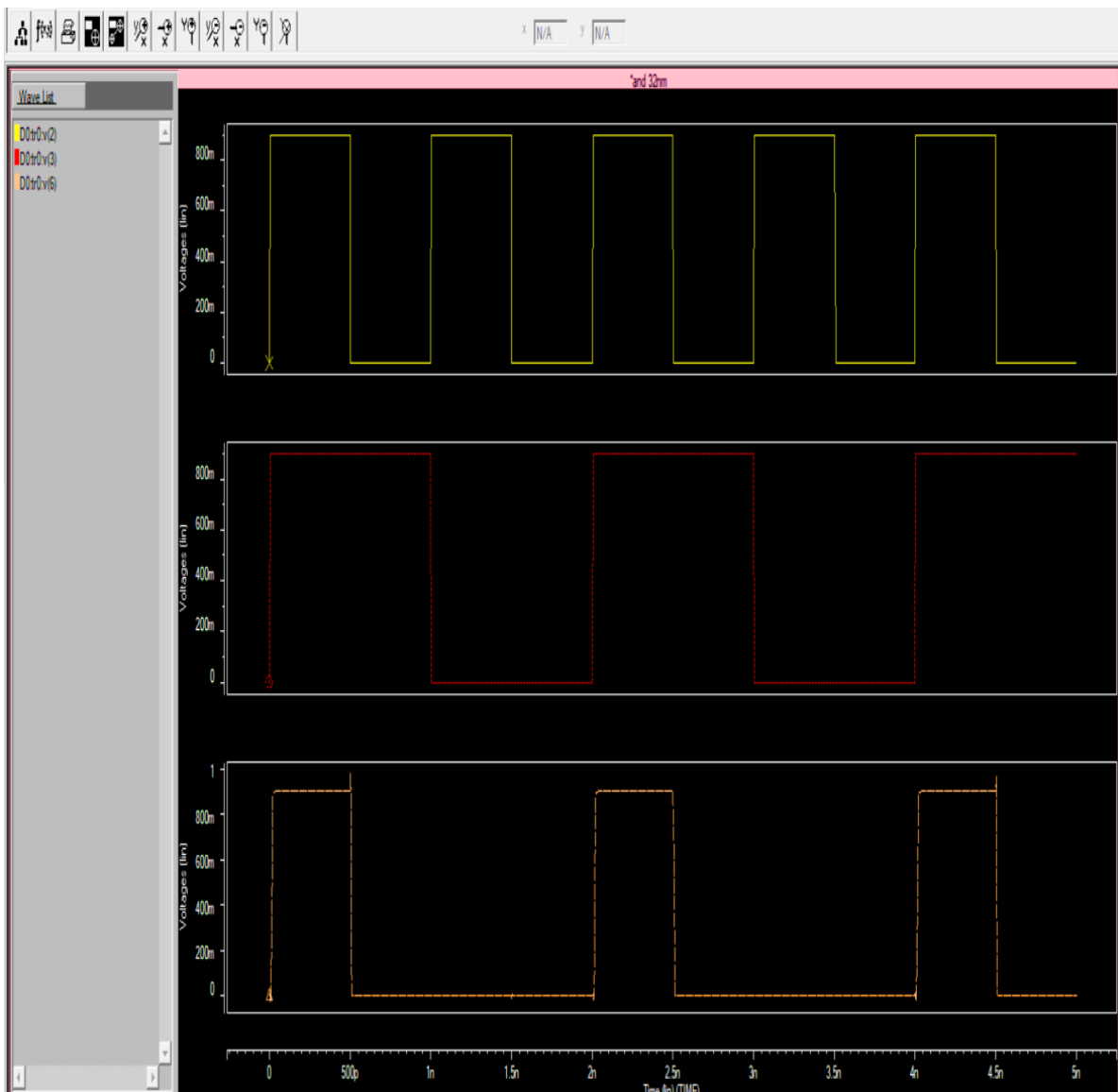


Fig 4.4 Simulation results for AND gate using 32nm MOSFET Technology

Figure 4.1.2 shows the simulation output of AND Gate 32nm MOSFET technology. The inputs given were v(2), v(3) and the output is taken by v(6).

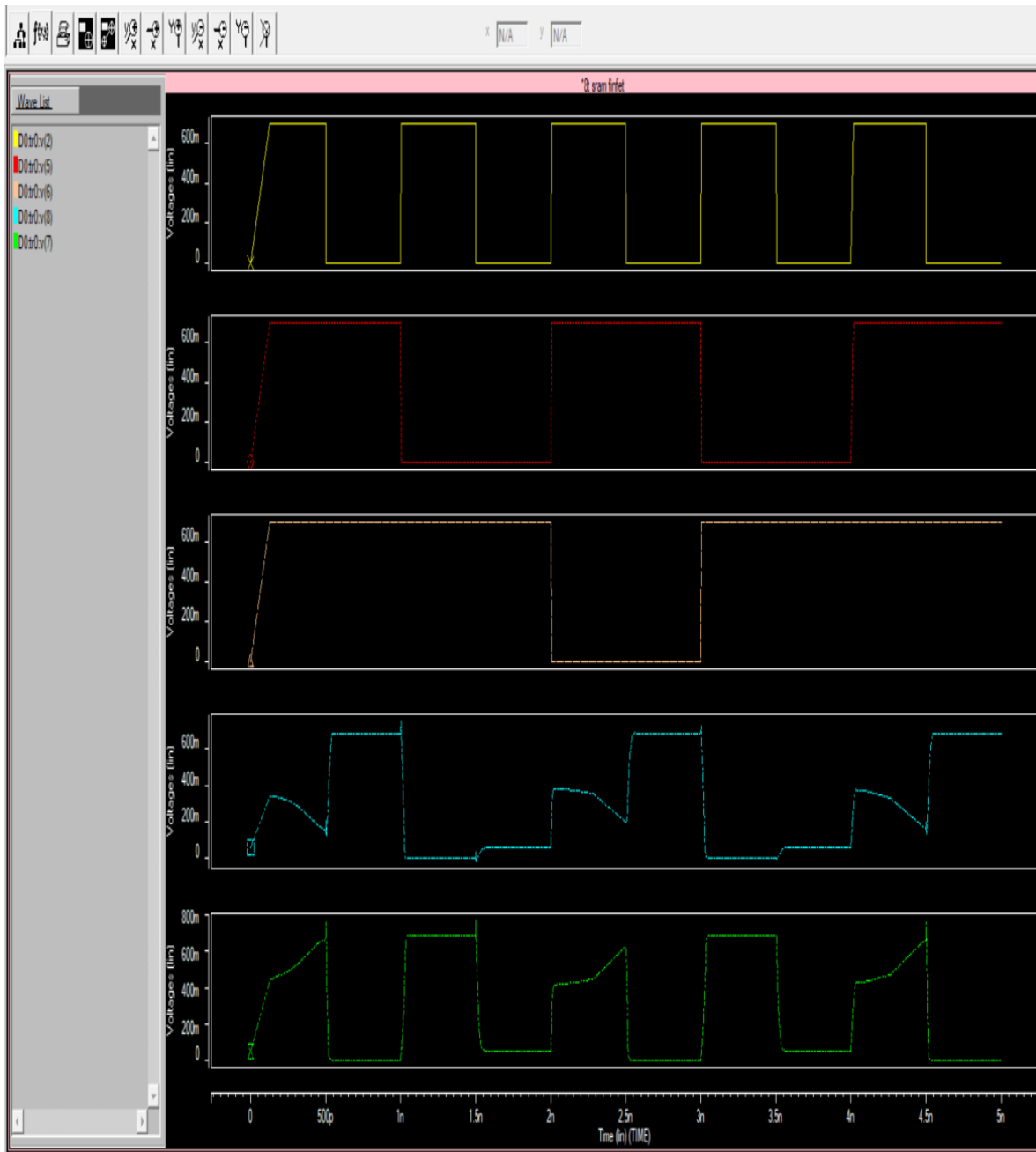


Fig 4.5: Simulation results for SRAM using 16nm GNRFET technology.

Figure 5.19 shows the simulation output of SRAM using 16nm GNRFET technology. The inputs given were v(2), v(5) and the output is taken by v(6), v(8), v(7).

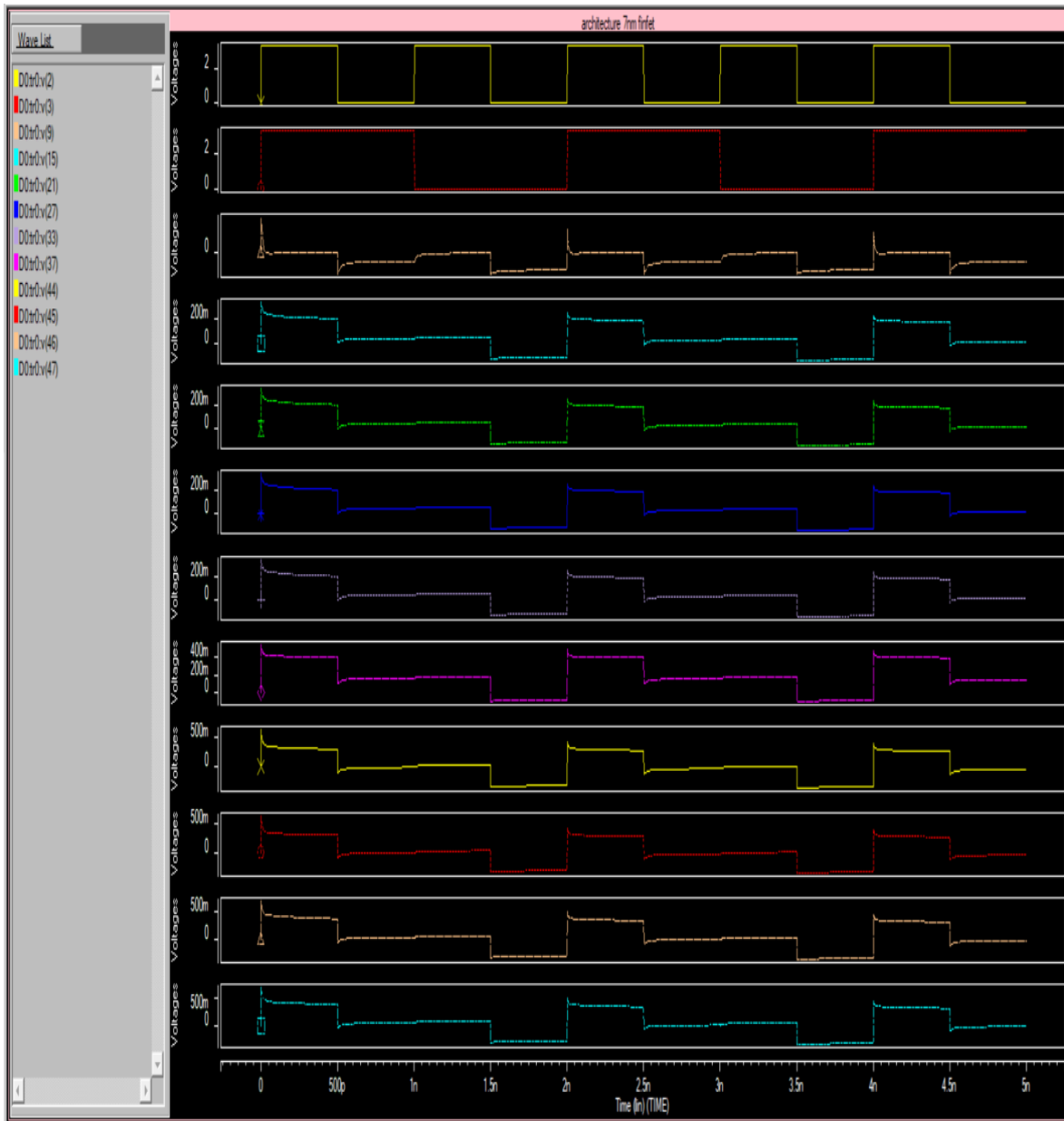


Fig 4.6: Simulation results for SRAM ARRAY ARCHITECTURE using 16nm GNR FET technology.

Figure 4.1.4 shows the simulation output of SRAM Array architecture using 16nm GNR FET technology. The inputs given were v(2), v(3) and the output is taken by v(9), v(15), v(21), v(27), v(33), v(37), v(44), v(45), v(46), v(47).

4.2 DC ANALYSIS OF SRAM ARCHITECTURE USING GNRFET TECHNOLOGY

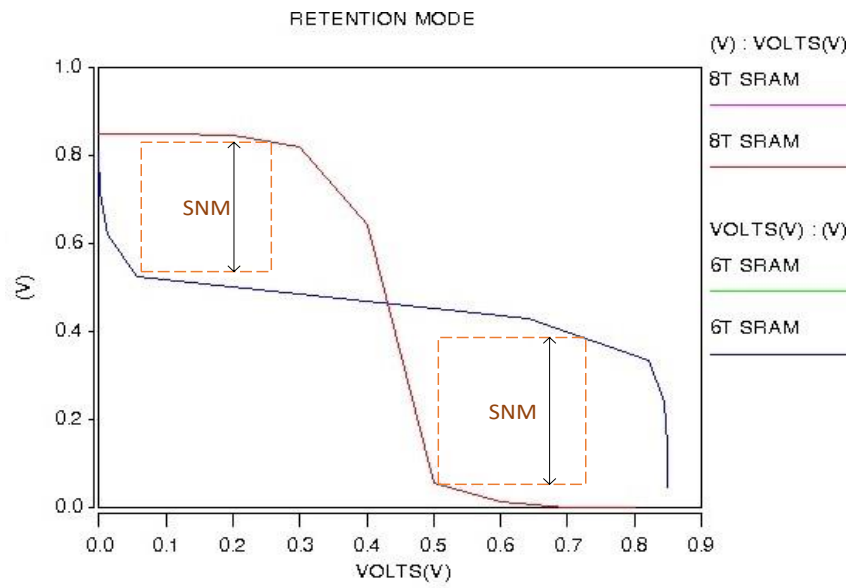


Fig 4.7: Butterfly curve of GNRFET-based SRAM architecture in retention mode

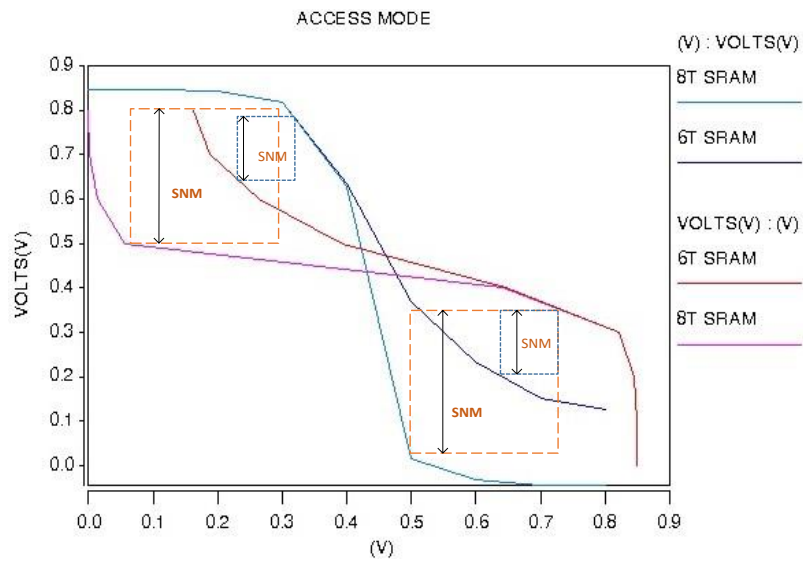


Fig 4.8: Butterfly curve of GNRFET-based SRAM architecture in access mode

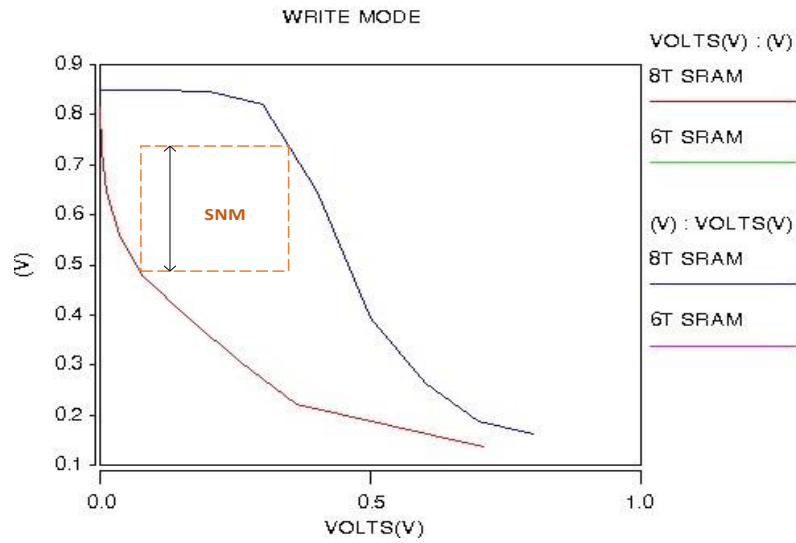


Fig 4.9 : Butterfly curve of GNRFET-based SRAM architecture in write mode

Table 4.2: Analysis for performance of GNRFET using 130nm

Device	130 nm		
	Power	Delay	PDP
ADDER	11.32×10^{-9}	478.35×10^{-12}	5.414×10^{-18}
AND	21.66×10^{-9}	498.87×10^{-12}	10.804×10^{-18}
DFF	51.34×10^{-9}	466.86×10^{-12}	23.968×10^{-18}
Proposed reconfigurable SRAM PUF cell	101.2×10^{-9}	344.7×10^{-12}	348.8×10^{-18}
MUX	195.2×10^{-9}	196.83×10^{-12}	38.421×10^{-18}
SRAM	121.12×10^{-9}	526.35×10^{-12}	637.45×10^{-18}

Table 4.3: Analysis for performance of GNRFET using 16 nm

Device	16 nm		
	Power	Delay	PDP
ADDER	7.603×10^{-9}	437.58×10^{-12}	3.326×10^{-18}
AND	11.45×10^{-9}	490.88×10^{-12}	5.62×10^{-18}
DFF	21.82×10^{-9}	427.46×10^{-12}	9.334×10^{-18}
Proposed reconfigurable SRAM PUF cell	81.15×10^{-9}	110.59×10^{-12}	89.974×10^{-18}
MUX	102×10^{-9}	107.44×10^{-12}	10.95×10^{-18}
SRAM	100.52×10^{-9}	428.25×10^{-12}	43.04×10^{-18}

CHAPTER 5

CONCLUSION AND FUTURE SCOPE

GNERFET is another promising substitute to remove the challenges and obstacles that are faced by conventional planar MOSFET in sub-100 nm technology. The usage of GNERFET has made further scaling of SRAM due to reduced random dopant fluctuation, steeper subthreshold slope, and relief of high-K material as gate oxide. We have performed simulation and analysis of Reconfigurable SRAM, SRAM array architecture by using 130 nm, 32 nm MOSFET technology and 7nm GNERFET technology. And compared the characteristics of both MOSFET and GNERFET Technology in terms of Power, Delay and Power Delay Product. The design and simulation of the SRAM model are accomplished in Synopsys HSpice tool based on 15nm technology. The simulation results reveal that the GNERFET-based 6T SRAM, 8T SRAM, SRAM Array Architecture cells show significant improvement in their performance with better stability and low-power consumption than mosfet based 6T SRAM cell, 8T SRAM cell and SRAM array architecture respectively.

This project also investigates on the stability performance in retention, read and write mode of 16nm GNERFET based 8T SRAM cell. A butterfly curve is extracted from the voltage transfer curve (VTC) of two cross-coupled GNERFET-based inverters to obtain and analyse the noise margin based on the read, write and retention operations. SNM acquired from the maximum square of the VTC of the inverter. There are two types of the SNM that affect the stability of the SRAM cell, namely, the write static noise margin (WSNM) and access static noise margin(ASNM). GNERFET, and MOSFET-based 8T SRAM cells improved access static noise margin considerably by 28%, and 20.5%, respectively, as well as average power consumption significantly by 99.05%, and 83.3%, respectively, to the GNERFET, and MOSFET-based 6T SRAM design. From the findings, It can be concluded that both GNERFET and MOSFET 8T SRAM cell gives better performance in Static Noise Margin (SNM) and power consumption than 6T SRAM cells.

REFERENCES

1. A. Babaei and G. Schiele, "Physical unclonable functions in the Internet of Things: State of the art and open challenges," *Sensors*, vol. 19, no. 14, p. 3208, Jul. 2019.
2. A. Maiti, J. Casarona, L. McHale, and P. Schaumont, "A large scale characterization of RO-PUF," in *Proc. IEEE Int. Symp. Hardw.-Oriented Secur. Trust (HOST)*, Jun. 2010, pp. 94–99.
3. B. Karpinsky, Y. Lee, Y. Choi, Y. Kim, M. Noh, and S. Lee, "physically unclonable function for secure key generation with a key error rate of $2E-38$ in 45nm smart-card chips," in *IEEE Int. Solid- State Circuits Conf. (ISSCC) Dig. Tech. Papers*, Jan. 2016, pp. 158–160.
4. C.-C. Chang and C.-J. Lin, "LIBSVM: A library for support vector machines," *ACM Trans. Intell.Syst. Technol.*, vol. 2, no. 3, pp. 1–27, Apr. 2011.
5. G. T. Becker, "The gap between promise and reality: On the insecurity of XOR arbiter PUFs," in *Cryptographic Hardware and Embedded Systems—CHES*, T. Güneysu and H. Handschuh, Eds. Berlin, Germany: Springer, 2015, pp. 535–555.
6. J. Shi, Y. Lu, and J. Zhang, "Approximation attacks on strong PUFs," *IEEE Trans. Comput.-Aided Design Integr. Circuits Syst.*, vol. 39, no. 10, pp. 2138–2151, Oct. 2020.
7. J. R. D. Kumar, C. G. Babu, V. R. Balaji, K. Priyadharsini, and S.P. Karthi, "Performance investigation of various SRAM Cells for IoT based wear-able biomedical devices," in *Inventive Communication and Computational Technologies*, G. Ranganathan, J. Chen, and Á. Rocha, Eds. Singapore: Springer, 2021, pp. 573–588.
8. J. Zhang and C. Shen, "Set-based obfuscation for strong PUFs against machine learning attacks," *IEEE Trans. Circuits Syst. I, Reg. Papers*, vol. 68, no. 1, pp. 288–300, Jan. 2021.
9. K. Agarwal and S. Nassif, "Statistical analysis of SRAM cell stability," in *Proc. 43rd ACM/IEEE Design Autom. Conf.*, Jul. 2006, pp. 57–62.
10. K.-U. Choi, S. Baek, J. Heo, and J.-P. Hong, "A 100% stable sense-amplifier-based physically unclonable function with individually embedded non-volatile memory," *IEEE Access*, vol. 8, pp. 21857–21865, 2020.
11. K. Xiao, M. T. Rahman, D. Forte, Y. Huang, M. Su, and M. Tehranipoor, "Bit selection algorithm suitable for high-volume production of SRAM-PUF," in *Proc. IEEE Int. Symp. Hardw.-Oriented Secur. Trust (HOST)*, May 2014, pp. 101–106.

12. L. Lin, S. Srivathsa, D. K. Krishnappa, P. Shabadi, and W. Burleson, "Design and validation of arbiter-based PUFs for sub-45-nm low-power security applications," *IEEE Trans. Inf. Forensics Security*, vol. 7, no. 4, pp. 1394–1403, Aug. 2012.
13. M. Bhargava, C. Cakir, and K. Mai, "Attack resistant sense amplifier based PUFs (SA-PUF) with deterministic and controllable reliability of PUF responses," in *Proc. IEEE Int. Symp. Hardw.-Oriented Secur. Trust (HOST)*, Jun. 2010, pp. 106–111.
14. M. Hiller, M.-D. Yu, and G. Sigl, "Cherry-picking reliable PUF bits with differential sequence coding," *IEEE Trans. Inf. Forensics Security*, vol. 11, no. 9, pp. 2065–2076, Sep. 2016.
15. M. Rostami, F. Koushanfar, and R. Karri, "A primer on hardware security: Models, methods, and metrics," *Proc. IEEE*, vol. 102, no. 8, pp. 1283–1295, Aug. 2014.
16. M. T. Rahman, A. Hosey, Z. Guo, J. Carroll, D. Forte, and M. Tehranipoor, "Systematic correlation and cell neighborhood analysis of SRAM PUF for robust and unique key generation," *J. Hardw. Syst. Secur.*, vol. 1, no. 2, pp. 137–155, Jun. 2017.
17. S. S. Kumar, J. Guajardo, R. Maes, G.-J. Schrijen, and P. Tuyls, "Extended abstract: The butterfly PUF protecting IP on every FPGA," in *Proc. IEEE Int. Workshop Hardw.-Oriented Secur. Trust*, Jun. 2008, pp. 6770.
18. T. McGrath, I. E. Bagci, Z. M. Wang, U. Roedig, and R. J. Young, "A PUF taxonomy," *Appl. Phys. Rev.*, vol. 6, no. 1, Mar. 2019, Art. no. 011303.
19. Y. Cao, W. Zheng, X. Zhao, and C.-H. Chang, "An energy-efficient current-starved inverter based strong physical unclonable function with enhanced temperature stability," *IEEE Access*, vol. 7, pp. 105287–105297, 2019.
20. Y. Gao, S. F. Al-Sarawi, and D. Abbott, "Physical unclonable functions," *Nature Electron.*, vol. 3, no. 2, pp. 81–91, 2020.