

HIGH SPEED LINEAR CONGRUENTIAL GENERATOR USING CNTFET TECHNOLOGY

Submitted in Partial fulfillment of the Requirements for the Award of
Bachelor of Engineering degree in Electronics and Communication

By

Sahithi P (40130171)

Yogapriya B (40130258)



**DEPARTMENT OF ELECTRONICS AND COMMUNICATION ENGINEERING
SCHOOL OF ELECTRICAL AND ELECTRONICS**

SATHYABAMA

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

CATEGORY -1 UNIVERSITY BY UGC

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

JEPPIAAR NAGAR, RAJIV GANDHI SALAI, CHENNAI - 600 119

APRIL – 2024



SATHYABAMA

INSTITUTE OF SCIENCE AND TECHNOLOGY
(DEEMED TO BE UNIVERSITY)

CATEGORY-I UNIVERSITY BY UGC

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 **Sahithi P(40130171)** and **Yogapriya B (40130258)** Who Carried out the project entitled "**HIGH SPEED LINEAR CONGRUENTIAL GENERATOR USING CNTFET TECHNOLOGY**" under my Supervision from November 2023 to April 2024.

Dr.Mathan N, M.Tech., Ph.D.

Internal Guide

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

Head of the Department

Submitted for Viva Voce Examination held on 18/04/2024.

Internal Examiner

External Examier

DECLARATION

We **Sahithi P(40130171)** and **Yogapriya B (40130258)** hereby declare that the Project Report entitled "**HIGH SPEED LINEAR CONGRUENTIAL GENERATOR USING CNTFET 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. *P.Sahithi*

2. *B.Yogapriya*

DATE: 18/04/2024

PLACE: CHENNAI

SIGNATURE OF THE CANDIDATES

ACKNOWLEDGEMENT

We are pleased to acknowledge our sincere thanks to The **Board of Management of Sathyabama Institute of Science and Technology** for their kind encouragement in doing this project and for completing it successfully. I am grateful to them.

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

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

In the era of technological advancements, information privacy safeguarding has become paramount across various sectors including defense, finance, and healthcare. Cryptography, a field requiring efficient data processing and secure storage, lies at the core of these security measures. Our project focuses on the optimization of Linear Congruential Generators (LCG), crucial for cryptographic applications and pseudorandom number generation. The implementation of LCG using Carbon Nanotube Field-Effect Transistor (CNTFET) technology has been pioneered by us, aiming to reduce leakage power through the innovative application of sleep techniques. This advanced approach represents a significant step towards minimizing energy consumption while simultaneously enhancing the overall performance and reliability of cryptographic systems. By integrating sleep modes into the CNTFET-based LCG design, leakage power is significantly curtailed without compromising the efficiency or output quality of the generator. The successful implementation and synthesis of this design, utilizing cutting-edge CNTFET technology, highlight the potential for substantial improvements in power efficiency while maintaining high standards of security and randomness essential for cryptographic algorithms.

TABLE OF CONTENTS

CHAPTER No.	TITLE	PAGE No.
	ABSTRACT	v
	LIST OF FIGURES	ix
	LIST OF TABLES	ix
	LIST OF SYMBOLS AND ABBREVIATIONS	x
1	INTRODUCTION	1
1.1	GENERAL INTRODUCTION	1
1.2	INTRODUCTION TO THREE OPERAND ADDERS	2
1.3	CMOS TECHNOLOGY	3
1.3.1	NMOS	4
1.3.2	PMOS	4
1.3.3	CMOS	4
1.3.4	CMOS LOGIC GATE	5
1.3.4.1	CMOS INVERTER	5
1.3.4.2	CMOS NAND GATE	6
1.4	MOSFET TECHNOLOGY	7
2	LITERATURE SURVEY	8
2.1	LITERATURE SURVEY	8
2.2	LITERATURE SUMMARY	17
2.3	PROBLEM STATEMENT	18

CHAPTER No.	TITLE	PAGE No.
3	AIM AND SCOPE OF THE PROJECT	19
	3.1 OBJECTIVES	19
	3.2 SCOPE OF THE PROJECT	20
4	EXISTING SYSTEM	21
	4.1 MDCLCG	21
	4.2 LCG	22
	4.3 CNTFET TECHNOLOGY	25
	4.3.1 DEVICE PARAMETERS OF CNTFET	26
	4.3.2 DEVICE PERFORMANCE OF CNTFET	27
5	PROPOSED SYSTEM	29
	5.1 SLEEP TECHNIQUE FOR LEAKAGE POWER REDUCTION IN LCG	29
6	RESULTS AND DISCUSSION	31
	6.1 SIMULATION RESULT OF EXISTING SYSTEM	31
	6.2 SIMULATION RESULT AND COMPARITIVE ANALYSIS OF PROPOSED SYSTEM	34
7	CONCLUSION	38
	7.1 CONCLUSION	38
	7.2 STANDARDS	39
	7.3 CONSTRAINTS	39
	REFERENCES	41

LIST OF FIGURES

FIGURE NO	FIGURE NAME	PAGE NO
1.1	NMOS Transistor	4
1.2	PMOS Transistor	4
1.3	CMOS Logic Gate	5
1.4	CMOS Inverter	6
1.5	CMOS Nand Gate	6
1.6	MOSFET Modes Diagram	7
4.1	MDCLCG Architecture	21
4.2	Block Diagram of LCG operation	23
4.3	General Circuit Diagram of LCG	24
4.4	CNTFET Diagram	28
6.1	LCG in 130nm MOSFET Technology	31
6.2	LCG in 32nm MOSFET Technology	32
6.3	LCG in 32nm CNTFET Technology	32
6.4	LCG with sleep technique in 130nm MOSFET Technology	35
6.5	LCG WITH SLEEP TECHNIQUE IN 32NM MOSFET TECHNOLOGY	35
6.6	LCG WITH SLEEP TECHNIQUE IN 32NM CNTFET TECHNOLOGY	36

LIST OF TABLES

TABLE No.	TABLE NAME	PAGE No.
4.1	DEVICE PARAMETERS OF CNTFET	27
6.1	COMPARISION ANALYSIS OF LCG UNDER 130NM, 32NM MOSFET AND 32NM CNTFET	33
6.2	COMPARISION ANALYSIS OF LCG WITH SLEEP TECHNIQUE UNDER 130NM,32NM MOSFET AND 32NM CNTFET	36

LIST OF ABBREVIATIONS

PRBG	Pseudo-random bit generator
LCG	Linear congruential generator
CLCG	Coupled LCG
MDCLCG	Modified dual CLCG
MOSFET	Metal-oxide-semiconductor field-effect- transistor
CNTFET	Carbon nano-tube field-effect transistor

CHAPTER-1

INTRODUCTION

1.1 GENERAL INTRODUCTION

In the realm of cryptographic systems, the paramount goal is to achieve optimal system performance while upholding robust security measures. Hardware implementations of cryptographic algorithms play a pivotal role in this endeavor, with modular arithmetic operations, including modular exponentiation, multiplication, and addition, serving as the cornerstone for various encryption techniques. The efficiency of these cryptographic algorithms is heavily reliant on the streamlined execution of these modular arithmetic operations.

Our paper elucidates the critical role of efficient hardware architecture in enhancing the performance of cryptographic operations, with particular emphasis on the implementation of Linear Congruential Generators (LCG) for pseudo-random bit generation. LCGs, integral to algorithms such as the modified dual-CLCG (MDCLCG), rely on fundamental arithmetic operations, notably binary addition, necessitating an effective implementation strategy. Distinctively, our project accentuates the MDCLCG as a secure and highly random pseudo-random bit generation method, capable of providing polynomial-time unpredictability for bit sizes exceeding 32 bits. However, the architecture of MDCLCG encounters challenges in scaling, particularly regarding area and critical path delay as operand size increases.

To address these challenges, our study introduces an innovative approach by employing Carbon Nanotube Field-Effect Transistor (CNTFET) technology for LCG implementation, alongside a comparative analysis with traditional MOSFET technology. Furthermore, we incorporate a sleep technique aimed at reducing leakage power, thereby enhancing the energy efficiency of our cryptographic hardware design. Our endeavor aims to advance the performance and security of pseudo-random bit generation in cryptographic applications, providing insights into the benefits of modern semiconductor technologies in cryptography.

1.2 INTRODUCTION TO THREE OPERANDS ADDERS

In the realm of cryptographic systems, the pursuit of optimal system performance while ensuring robust security measures remains paramount. Hardware implementations of cryptographic algorithms assume a pivotal role in this pursuit, with modular arithmetic operations—such as modular exponentiation, multiplication, and addition—forming the bedrock for various encryption techniques. The efficiency of these cryptographic algorithms is contingent upon the streamlined execution of modular arithmetic operations.

Our study elucidates the criticality of efficient hardware architecture in bolstering the performance of cryptographic operations, with a specific focus on the implementation of Linear Congruential Generators (LCG) for pseudo-random bit generation. LCGs, which constitute the cornerstone of algorithms like the modified dual-CLCG (MDCLCG), rely on fundamental arithmetic operations, particularly binary addition, necessitating an effective implementation strategy. Our project accentuates the MDCLCG as a secure and highly random pseudo-random bit generation method, capable of providing polynomial-time unpredictability for bit sizes exceeding 32 bits. However, the architecture of MDCLCG encounters scaling challenges, particularly concerning area and critical path delay as operand size escalates.

To tackle these challenges, an innovative approach is introduced in our study, employing Carbon Nanotube Field-Effect Transistor (CNTFET) technology for LCG implementation, accompanied by a comparative analysis with traditional MOSFET technology. Additionally, we incorporate a sleep technique aimed at reducing leakage power, thereby enhancing the energy efficiency of our cryptographic hardware design. The endeavor seeks to advance the performance and security of pseudo-random bit generation in cryptographic applications, providing insights of the benefits of modern semiconductor technologies in cryptography.

The three-operand binary addition, a primary arithmetic operation in LCG-based pseudo-random bit generators (PRBG), such as coupled LCG (CLCG), MDCLCG, and coupled variable input LCG (CVLCG), is pivotal in cryptographic

systems. The MDCLCG emerges as the most secure and highly random PRBG method, yet its hardware architecture poses challenges due to the linear increase in area and critical path delay with operand size. Therefore, enhancing the performance of MDCLCG necessitates an efficient implementation of the three-operand adder. Consequently, a novel high-speed, area-efficient adder technique is proposed, leveraging pre-compute bitwise addition followed by carry-prefix computation logic. This approach aims to minimize gate area consumption and propagation delay, offering a promising avenue for improving the performance of cryptographic systems. Additionally, the proposed adder architecture undergoes implementation using Verilog HDL and synthesis with a commercially available 32nm CMOS technology library, enabling comprehensive evaluation against existing adder techniques.

1.3 CMOS TECHNOLOGY

CMOS technology, an integral aspect of integrated circuit manufacturing, derives its name from "Complementary Metal Oxide Semiconductor." This technology finds widespread application across various electronic components such as microprocessors, batteries, and digital sensors, owing to numerous inherent advantages. Utilizing both NMOS and PMOS, CMOS technology realizes diverse logic functions, ensuring that N and P MOSFET channels exhibit matching characteristics. Before the advent of CMOS, PMOS and NMOS logic represented prevalent approaches for implementing logic gates. However, NMOS technology gradually supplanted PMOS, initially being the standard IC fabrication method. Initially, CMOS technology lagged behind NMOS in terms of speed and cost efficiency. Nonetheless, CMOS technology's advantages over NMOS, such as minimized power dissipation and enhanced performance due to reduced static power dissipation, have significantly mitigated these disparities. By minimizing power dissipation solely during circuit switching, CMOS technology facilitates superior performance and the integration of more CMOS gates on an IC, thereby enhancing functional density and manufacturing efficiency.

1.3.1 NMOS

An N-channel MOSFET consists of an N-type source and drain diffused onto a P-type substrate, where electrons serve as the majority carriers. When a sufficiently high voltage is applied to the gate, the NMOS conducts, while it remains non-conductive otherwise. Because electrons exhibit faster mobility compared to holes, NMOS devices are typically acknowledged for their faster operation in contrast to PMOS counterparts.

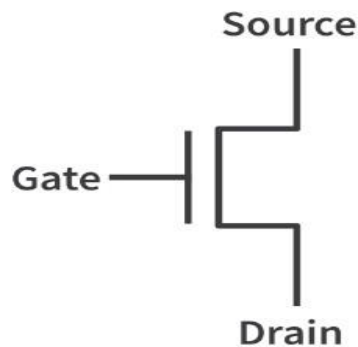


Fig 1.1 NMOS Transistor

1.3.2 PMOS

In a P-channel MOSFET, the Source and Drain are diffused on a substrate, with the Source being P-type and the substrate being N-type, resulting in holes being the majority carriers. PMOS conducts when subjected to a low voltage, while it remains non-conductive under high gate voltage.

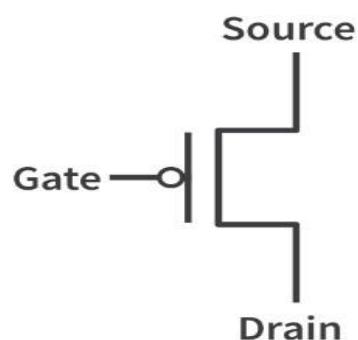


Fig 1.2 PMOS Transistor

1.3.3 CMOS

In CMOS technology, logic functions are devised using both N-type and P-type transistors. When one type of transistor is activated, it concurrently deactivates the other, eliminating the need for pull-up resistors and favoring the

utilization of simple switches. Within CMOS logic gates, N-type MOSFETs establish a pull-down network between the output and the low voltage supply rail (VSS or ground), whereas P-type MOSFETs form a pull-up network between the output and the higher-voltage rail (often VDD). As a result, when the P-type MOSFET is deactivated, the N-type MOSFET is activated, and vice versa, ensuring that only one network is active while the other remains inactive for any given input pattern. CMOS offers advantages such as high speed, low power dissipation, high noise margins in both states, and a wide range of source and input voltages with a fixed source voltage.

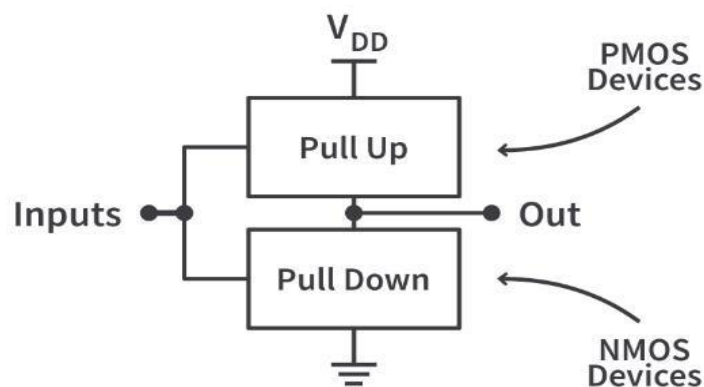


Fig 1.3 CMOS Logic Gate

1.3.4 CMOS LOGIC GATE

1.3.4.1 CMOS INVERTER

The CMOS inverter represents the simplest form of CMOS logic gate, comprising both PMOS and NMOS FET. Input A acts as the gate voltage for both transistors, while Y denotes the output. The NMOS transistor receives its input from VSS or ground, whereas the PMOS transistor receives its input from VDD. When the input (A) is at a low voltage level ($<V_{DD}$, approximately 0 V, corresponding to Logic 0), the NMOS is in the OFF state, while the PMOS is in the ON state. Consequently, VDD is observed at the output through the path of the P-channel MOSFET, resulting in a high output (Logic 1) as the circuit is pulled up to VDD. Conversely, when the input is at a high voltage level ($\sim V_{DD}$, corresponding to Logic 1), the PMOS is in the OFF state, whereas the NMOS is in the ON state.

This configuration causes the output to be pulled down, yielding a low output (Logic 0).

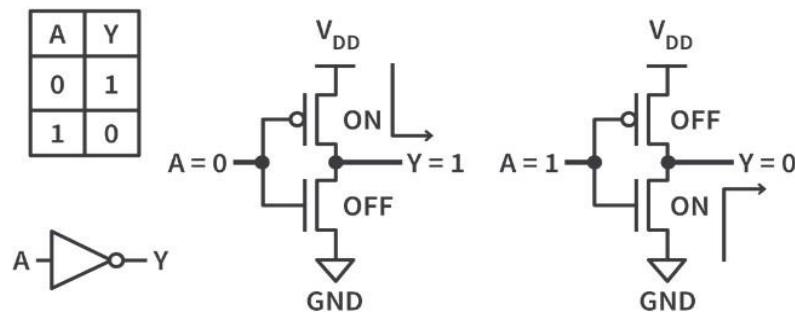


Fig 1.4 :CMOS Inverter

1.3.4.2 CMOS NAND GATE

A 2-input NAND gate has two N-channel MOSFETs connected in series between Y (output) and GND and two P-channel MOSFETs connected in parallel between V_{DD} and Y.

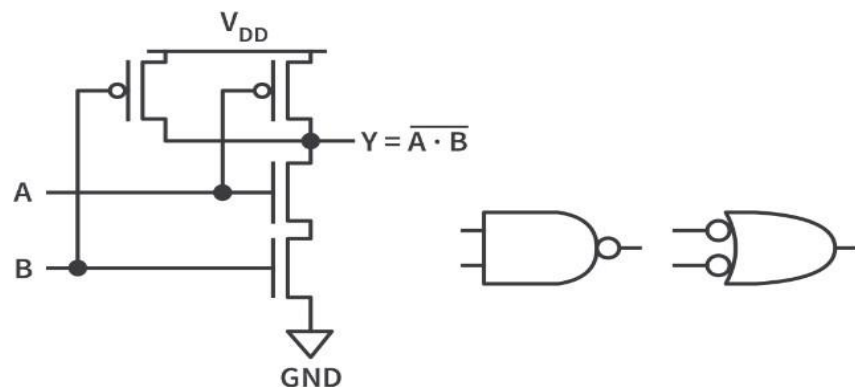


Fig 1.5 :CMOS Nand Gate

If either A or B is low (Logic 0), at least one of the NMOS transistors will be OFF. In this configuration, the path from Y to GND is interrupted when the NMOS transistors are connected in series. However, with at least one of the PMOS transistors ON, a path from Y to V_{DD} is established, resulting in a high output (Logic 1). To obtain a low output (Logic 0) at Y, both A and B must be high to ensure that both NMOS transistors are ON, thus completing the path from Y to GND. In all other input combinations, Y remains high.

1.4 MOSFET TECHNOLOGY

MOSFETs, known as Metal-Oxide-Semiconductor Field-Effect Transistors, are essential components in various electronic circuits due to their tri-terminal, unipolar, and voltage-controlled nature, coupled with their high input impedance. These devices find application across a spectrum of electronic systems, serving as inverters, integral parts of digital circuits, passive elements, high-frequency amplifiers, and key components in motor drives, electronic relays, switch-mode power supplies (SMPS), and as switches.

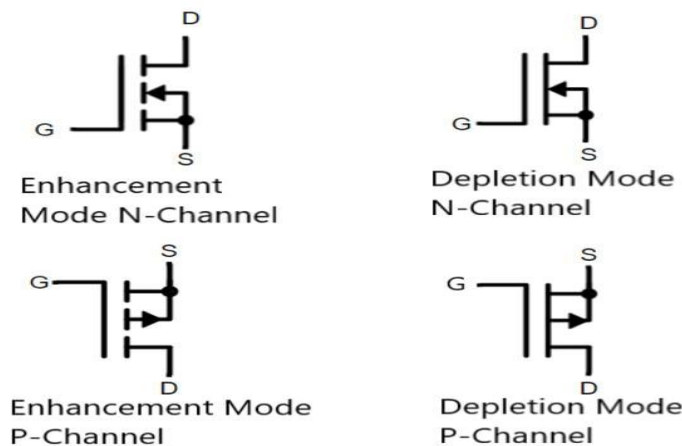


Fig 16 MOSFET Modes Diagram

In a typical common-source MOSFET configuration, the drain terminal acts as the output, carrying the transistor's output signal. By applying a voltage to the gate terminal, an electric field is generated, controlling the flow of current between the source and drain terminals. This control mechanism enables MOSFETs to regulate current flow effectively, making them pivotal in circuit design and operation. Depletion-mode MOSFETs feature an established channel, allowing current conduction even without applied gate voltage. Typically, these transistors remain closed in the absence of bias voltage at the gate terminal. However, as the gate voltage increases positively, the channel width in depletion mode expands, facilitating current flow through the device.

CHAPTER-2

LITERATURE SURVEY

2.1 LITERATURE SURVEY

K. Panda and K. C. Ray et.al., (2019) [1] The utilization of pseudorandom bit generators (PRBGs) holds paramount importance in the realm of securing data during its transmission and storage within various cryptographic applications. Among the plethora of existing PRBG methodologies, the dual-coupled LCG (dual-CLCG) method has garnered notable recognition owing to its heightened security measures, predominantly reliant on inequality comparisons to generate pseudorandom bits at irregular intervals. Nonetheless, prevailing dual-CLCG architectures confront inherent limitations, including excessive memory consumption, elevated initial clock latency, and the inability to attain maximum length sequences. In response to these challenges, this paper introduces a novel PRBG approach dubbed "modified dual-CLCG," accompanied by a sophisticated very large-scale integration (VLSI) architecture. This innovative framework aims to streamline the generation of pseudorandom bits by enforcing a uniform clock rate with minimal hardware complexity, facilitated by the integration of carry-save adder techniques for optimized three-operand addition. Executed using Verilog HDL and prototyped on commercially available FPGA devices, this proposed architecture represents a pivotal stride forward in PRBG technology, poised to deliver heightened security and efficiency across cryptographic domains.

A.K. Panda and K. C. Ray et.al., (2018) [2], The imperative need for hardware security in Internet-of-Things (IoT) applications necessitates the development of a pseudorandom bit generator (PRBG) characterized by low hardware area, high speed, and robust cryptographic security. Among the various PRBGs, the Blum-Blum-Shub (BBS) method stands out as cryptographically secure due to its reliance on the large prime factorization problem. However, the computational expense associated with the BBS method arises from its dependency on large integer modular multiplication. To address this challenge, this paper introduces a modified radix-2 iterative Montgomery modular multiplier

tailored for the efficient hardware implementation of a 1024-bit BBS generator. This novel approach replaces two two-operand adders with a single three-operand adder, thereby enhancing computational efficiency. Moreover, the critical path delay is mitigated by employing a fast parallel prefix Han-Carlson adder for three-operand addition, further optimizing performance. Implemented using Verilog HDL and prototyped on the Virtex5 FPGA device, the proposed architecture demonstrates the capability to operate at a maximum frequency, underscoring its suitability for IoT security applications.

Rezai and P. Keshavarzi et.al., (2015) [3], Modular exponentiation, In various public-key cryptosystems, modular exponentiation is a fundamental operation, often involving repetitive modular multiplications, especially when dealing with large modulus and exponent values. Montgomery modular multiplication, commonly employed for quotient relaxation, utilizes carry-save adders to minimize critical path delays. This study presents and evaluates a novel and efficient Montgomery modular multiplication architecture based on a novel digit serial computation approach. This innovative architecture simplifies high-radix partial multiplication to binary multiplication, enabling multiple multiplications of consecutive zero bits within a single clock cycle. Additionally, modifications to both right-to-left and left-to-right modular exponentiation architectures integrate the proposed modular multiplication architecture as their structural unit. Experimental results on a Xilinx Virtex 5 FPGA demonstrate significantly improved total computation time and throughput rates compared to existing literature, underscoring the effectiveness of the proposed architectures in cryptographic operations.

K. S. Pandey, D. K. B. N. Goel, and H. Shrimali et.al., (2019) [4], Parallel prefix adders stand as one of the most prevalent arithmetic units, having undergone extensive investigation across various design levels, including architecture, register transfer level (RTL), gate level, circuit level, and layout level. This paper contributes significantly to the comprehension of these adders in two key ways. Firstly, it endeavors to articulate various parallel prefix adders through elegant and consistent formulations, aiming to provide clarity and coherence in

understanding. Secondly, the paper introduces a novel family of parallel prefix adders at the architecture level, accompanied by estimates of their area-throughput characteristics. While the speeds achieved by this new family align with those of state-of-the-art adders, their area characteristics exhibit improvements over existing ones, albeit with a slightly higher level of hardware complexity.

S. S. Erdem, T. Yanik, and A. Celebi et.al., (2017) [5], This paper introduces a highly efficient hardware architecture designed specifically for the Montgomery algorithm, a fast modular multiplication technique widely used in cryptographic applications. By employing carry-save adders to accumulate partial products and bypass carry propagation delays, the study explores digit-serial implementations of the Montgomery algorithm, with a particular emphasis on handling large integers. Through thorough analysis, the paper provides a detailed examination and a strict upper bound for intermediate results generated during digit-serial computation. Based on this analysis, the study proposes an optimized digit-serial Montgomery modular multiplier architecture utilizing carry-save adders, highlighting its complexity. Notably, the architecture incorporates pipelined carry select adders to perform two essential tasks: aggregating carry-save vectors representing the modular product and conducting subtraction of the modulus from this aggregated result if further reduction is necessary.

S.-R. Kuang, J.-P. Wang, K.-C. Chang, and H.-W. Hsu et.al., (2013) [6], In the Rivest, Shamir, and Adleman (RSA) cryptosystem, modular exponentiation often involves repeated modular multiplications on large integers to accomplish encryption or decryption tasks. To expedite this process, numerous high-speed Montgomery modular multiplication algorithms and hardware architectures integrate carry-save addition techniques to circumvent carry propagation delays inherent in traditional add-shift loops. This paper introduces an energy-efficient algorithm and its corresponding architecture aimed at reducing energy consumption while concurrently enhancing the throughput of Montgomery modular multipliers. The proposed architecture streamlines operations by circumventing unnecessary carry-save addition and register write operations, thereby diminishing energy consumption and boosting throughput. Additionally, modifications are

made to the barrel register full adder (BRFA) to facilitate the application of the gated clock design technique, further reducing energy consumption associated with storage elements in BRFA. Experimental results corroborate the efficacy of the proposed approach in terms of energy efficiency and throughput improvement.

S.-R. Kuang, K.-Y. Wu, and R.-Y. Lu et.al., (2016) [7], In this paper, a novel Montgomery multiplication algorithm is proposed, aiming to achieve a low-cost and high-performance Montgomery modular multiplier implementation. The proposed algorithm operates on binary data representation, utilizing only a one-level carry-save adder (CSA) to mitigate carry propagation delays typically encountered in addition operations. This CSA also serves for operand pre-computation and format conversion from the carry-save format to binary representation, resulting in reduced hardware costs and shorter critical path delays, albeit with additional clock cycles required for completing each modular multiplication. To address this trade-off, a configurable CSA (CCSA) is introduced, allowing for the reduction of extra clock cycles by half through the implementation of one full adder or two serial half-adders. Furthermore, a mechanism is developed to detect and bypass unnecessary carry-save addition operations within the one-level CCSA architecture while maintaining short critical path delays. Consequently, the additional clock cycles for operand pre-computation and format conversion can be concealed, leading to enhanced throughput. Experimental results demonstrate that the proposed Montgomery modular multiplier achieves superior performance and substantial improvements in area-time product compared to prior designs.

Gagan Abbot and Dhruv Sharma et.al., (2020) [8], The focus of this paper lies in the VLSI architecture design of DSP, particularly emphasizing the development of dedicated systems for signal processing, image processing, and various communication applications. Through the utilization of VLSI design techniques and systolic architectures, the study aims to explore the trade-offs between speed, area, and power across different DSP applications. While memory-based structures have traditionally been favored for signal processing tasks involving multiplication with specific coefficient sets, this paper introduces a novel memory-based approach. This approach offers advantages in terms of

reduced latency and area, particularly in scenarios where memory processing time surpasses the computation time typical of traditional multipliers. The key innovation lies in lookup table (LUT) optimization, which effectively reduces both area and power consumption. Additionally, the paper introduces a pipelined version of the memory-based multiplier, further mitigating combinational path delays.

Sudipta Bose, Arijit De, and Indrajit Chakrabarti et.al., (2021) [9], In real-time seismic-alert systems, finite impulse response (FIR) filters necessitate low complexity, high speed, and re-configurability. To meet these requirements, this study employs the common sub-expression elimination (CSE) technique, recognized for reducing hardware complexity by minimizing logic operators (LOs) and logic depths (LDs) within digital FIR filters. Introducing a novel matrix grouped CSE (MCSE) algorithm, this work outperforms existing CSE methods in LOs and LDs minimization. Additionally, it introduces a new half-unit biased (HUB) based rounding technique to mitigate truncation error while maintaining low complexity and utilizes cut-set retiming to reduce critical-path-delay (CPD). Two hardware-efficient FIR filter architectures (I and II) are presented, incorporating the proposed canonical signed digit (CSD) based MCSE algorithm, HUB rounding, and cut-set retiming approach. Architecture II represents a hardware-efficient realization of a reconfigurable FIR filter. Hardware implementations on FPGA and ASIC platforms demonstrate significant reductions: architecture I achieves over 25%, 49%, 38%, 36%, and 31% reduction in LOs, CPD, effective latency, area-delay-product (ADP), and power-delay-product (PDP), respectively, compared to state-of-the-art CSE-based architectures. Architecture II exhibits nearly 48%, 12%, and 13% reduction in CPD, ADP, and PDP over its counterpart.

Tresa Joseph, Bindiya T. S et.al., (2021) [10], This paper presents a novel technique utilizing multiplexers to accelerate matrix vector multiplication (MVM) within long short-term memory networks. By employing multiple constant multiplication with separate generation and selection of partial products, the proposed architecture drastically reduces implementation complexity in terms of cell area and power efficiency. An effective truncation method is employed to

ensure reductions in hardware complexity and power consumption. Instead of shifting, inner product computations benefit from input coefficient truncation, enabling the use of combinational circuits over sequential designs. Furthermore, to improve the overall clock period, a new design for inner product computations is introduced, leveraging a modified multiplexer architecture. Experimental results demonstrate a significant reduction in MVM implementation complexity alongside a noteworthy 14% decrease in power consumption.

Amit Kumar Panda, Rakesh Palisetty, and Kailash Chandra Raym et.al.,(2020) [11] ,A three-operand binary adder serves as the fundamental unit for performing modular arithmetic in various cryptography and pseudorandom bit generator (PRBG) algorithms. While the carry-save adder (CS3A) is a commonly utilized technique for three-operand addition, its ripple-carry stage results in a high propagation delay of $O(n)$. Alternatively, a parallel prefix two-operand adder like the Han-Carlson (HCA) can be employed for three-operand addition, significantly reducing the critical path delay albeit at the expense of additional hardware. Therefore, a novel high-speed and area-efficient adder architecture is proposed, utilizing pre-compute bitwise addition followed by carry-prefix computation logic to execute the three-operand binary addition. This approach consumes substantially less area, exhibits low power consumption, and dramatically reduces the adder delay to $O(\log_2 n)$. The proposed architecture is validated functionally on an FPGA device and synthesized with a commercially available 32nm CMOS technology library. Post-synthesis results of the proposed adder demonstrate performance improvements of 3.12, 5.31, and 9.28 times compared to the CS3A for 32-bit, 64-bit, and 128-bit architectures, respectively. Moreover, it exhibits smaller area, lower power dissipation, and reduced delay compared to the HC3A adder. Additionally, the proposed adder achieves the lowest area-delay product (ADP) and power-delay product (PDP) among existing three-operand adder techniques.

Guilherme Paim, and Sergio Bampi et.al., (2021) [12], Efficient Kalman filter (KF) designs are crucial for real-time mobile applications like nano-drone navigation, robots' localization, and spacecraft orbit control. The KF involves complex matrix operations, especially within the Kalman gain (KG)

function, requiring matrix inversions, determinant calculations, and division operations. This article presents an architectural approach that balances conflicting low-power and high-performance requirements for real-time KF processing. Through a combination of architectural solutions, our exploration reveals that semi-parallel and sequential KF architectures offer the best balance of circuit area, power dissipation, and processing speed. Compared to existing solutions, our architecture demonstrates higher efficiency, requiring significantly fewer arithmetic operators and clock cycles. Simulations of system identification, noise elimination, and state estimation applications showcase the effectiveness of our KF architecture, achieving speedy adaptation, precision in noise elimination, and reliability in state estimation processes.

Nikhil Advait Gudala, Trond Ytterdal, and John J. Lee et.al., (2021) [13], One of the significant areas of research in VLSI focuses on designing power-efficient and high-speed data path logic systems, with digital adders being particularly crucial. The propagation delay of a carry through the adder limits the speed of addition in digital adders. Carry Select Adder (CSLA) addresses this issue by generating multiple carry bits and selecting one for the desired output, yet it lacks area efficiency due to its use of Ripple Carry Adders (RCA) pairs. This study proposes using Binary to Excess-1 Converter (BEC) instead of RCA in the regular CSLA to achieve high speed and low power consumption. Performance evaluations of three adders, conventional CSA, CSA with RCA, and CSA with BEC, are conducted and compared. The results demonstrate that while the delay of CSA and CSA with RCA remains the same, there's a notable reduction in area and power when using CSA with BEC, with approximately 18.67% reduction in area and 25.85% reduction in power compared to CSA with RCA. All simulations were performed using 45nm technology.

Spoorthi H R and Dr. Narendra C P et.al., (2019) [14], This paper introduces a high-speed, low-power data path architecture for a Multiply–Accumulate (MAC) unit utilizing the Baugh–Wooley multiplier along with the 4:2 Compressor. Typically, the MAC unit comprises Partial-Product Generation terms (PP unit) and a reduction tree in the first stage, followed by an

accumulation stage of an adder with sign extension. By operating the proposed architecture at a lower frequency, gates can be downsized within the available time slack, leading to reductions in power consumption, delay, and area. A novel MAC architecture with a compressor is proposed, capable of efficiently performing multiply-accumulate or multiply operations for N-bit operands. The proposed architecture is implemented using the ISE Xilinx Plan Ahead tool 14.7 and Cadence RTL compiler, with a comparison provided against Ripple Carry Adder, Carry Save Adder, and Brent-Kung Adder architectures.

Abhiram T, Ashwin T, Sivaprasad B, Aakash S, Anita J.P et.al., (2017) [15], In VLSI system design, key considerations such as power consumption, delay, and area utilization are critical factors. Carry Select Adders (CSLAs) are widely favored in data processing processors for their ability to perform fast arithmetic functions, making them instrumental in high-speed data processing applications. Compared to conventional adders, CSLAs exhibit superior performance in terms of speed. Notably, the structure of CSLA presents opportunities for area reduction, prompting a gate-level modification approach. This paper introduces modifications at the gate level for regular CSLA, leading to the design of 16-bit, 32-bit, 64-bit, and 128-bit SQRD CSLAs. Comparative analysis between the regular and modified CSLA configurations reveals notable reductions in both area and power consumption. The proposed approach advocates for the adoption of simple, optimized, and efficient gate-level modifications, which result in significant area and power savings for CSLAs, albeit with a marginal increase in delay.

K. Pavan , P. Rahul Reddy et.al., (2021) [16], This paper introduces a novel approach to designing a comparator with N bits, aiming to optimize area utilization while achieving high-speed operation with minimal power dissipation. The proposed digital comparator facilitates scalability of area and power requirements, achieved through a bitwise comparison from the least significant bit to the most significant bit. Utilizing a parallel prefix tree structure, comparisons are conducted only when bits are unequal, thus enhancing efficiency. The architecture comprises two distinct modules: the Comparison Evaluation Unit (CEU) and the Final Unit (FU), which work independently to

validate comparison results based on CEU outcomes. Leveraging structured VLSI methodology, the proposed architecture allows for area estimation through analytical methods, correlating transistor count and total delay with operand bit width. Spectre simulations conducted at 1 GHz using 0.18-micron CMOS technology demonstrate significant improvements over existing models, with a 77.76% reduction in power consumption and a 31.92% increase in operating speed.

Dinesh Kumar Saini, Shwetha Meena, (2015) [17], This paper presents a novel approach to designing a 16-bit Binary Coded Decimal (BCD) adder, integrating power gating design, dual threshold voltage (DVT), and the LECTOR technique. The continuous scaling of devices to achieve higher density, lower power consumption, and enhanced performance has led to a notable increase in leakage power dissipation. At nanometer-scale technologies, approximately 30% of total power dissipation is attributed to leakage power. The objective of this study is to analyze and compare static power reduction techniques, including power gating, DVT, and LECTOR. Performance metrics such as average power dissipation and delay are evaluated for each technique using 1-bit full adders implemented with CMOS logic. The circuit design is realized using Cadence Virtuoso tools in 180-nanometer technology.

Habib Muhammad Nazir Ahmad, Mohammad Shafquatul Islam, Kazi Muhammad Jameel, Arman Riaz Ochi, Rakibul Hafiz (2014) [18], This paper presents a comparative analysis of 12-CNTFET and GDI CNTFET-based full adder implementations at the 32 nm level, focusing on stability, power dissipation, and Power Delay Product (PDP) as key performance metrics. Through intensive HSPICE simulations, the power and delay distributions of these CNTFET-based full adders are thoroughly investigated. The results indicate a noticeable reduction in short current power consumption for both circuits, with the GDI CNTFET exhibiting superior performance in terms of power consumption and PDP variations. Furthermore, the CNTFET-based one-bit Full Adder cell demonstrates enhanced tolerance to Process, Voltage, and Temperature (PVT) variations compared to its CMOS counterpart.

Rajendra Prasad S, Madhavi B K, Lal Kishore K(2012) [19] , In the pursuit of maintaining historical delay reduction while curbing active power dissipation, the scaling down of both VDD and V_t in semiconductor technology has become imperative. However, the scaling of V_t precipitates a significant upsurge in sub-threshold leakage power, emerging as a substantial constituent of total power dissipation, now dominating the power consumption landscape in processor hardware and software design. Carbon nanotubes offer a promising alternative to CMOS with their superior properties. Addressing the prevalent issue of leakage power in high-performance microprocessors, particularly in caches implemented using SRAM cells, this paper introduces a novel circuit-level state-saving ultra low-leakage technique tailored for CNTFET-based SRAM Cells. Demonstrating remarkable efficacy, the proposed technique achieves a 96% reduction in leakage power compared to conventional CNTFET SRAM cells, while maintaining minimal area and delay trade-offs.

Rajendra Prasad S, Madhavi B K, Lal Kishore K(2012) [20] , In the context of advancing semiconductor technology, the reduction of both VDD and V_t is essential to uphold historical delay reduction while mitigating active power dissipation. However, the downsizing of V_t leads to a significant surge in sub-threshold leakage power, now constituting a substantial portion of total power dissipation and emerging as the primary concern in processor hardware and software design. Carbon nanotubes present themselves as a promising alternative to CMOS due to their superior properties. Addressing the significant power consumption issue in high-performance microprocessors, particularly in caches employing SRAM cells, this paper introduces a novel circuit-level state-saving ultra-low-leakage technique tailored specifically for CNTFET-based SRAM cells. The proposed technique achieves an impressive 96% reduction in leakage power compared to conventional CNTFET SRAM cells, while maintaining minimal area and delay trade-offs.

2.2 LITERATURE SUMMARY

To implement the Modified Dual-CLCG, the chosen three-operand carry-save adder offers reduced delay but increases area consumption. Conversely, the Han-Carlson adder, utilized in the proposed parallel prefix architecture,

boasts lower delay but comes with a drawback of increased area usage. Meanwhile, employing a carry-save adder in Montgomery modular multiplication trades off higher critical path delay for reduced area. Various parallel prefix adder designs, such as the Ling adder and Weinberger-Smith Recurrence, offer differing trade-offs between delay and area. For Multiply-Accumulate (MAC) units, utilizing a Baugh-Wooley multiplier and a 4:2 compressor yields a high-speed, low-power data path architecture. To mitigate carry propagation delay, the Carry Select Adder (CSLA) generates multiple carry bits and selects the desired output. This study introduces the use of a Binary to Excess-1 Converter (BEC) instead of a regular RCA in the CSLA, enhancing speed and power efficiency. Additionally, multiple constant multiplication with separate generation and selection of partial products is utilized for design, resulting in reduced implementation complexity in terms of cell area and power efficiency. To further enhance power reduction, the incorporation of sleep techniques into the existing LCG system is proposed.

2.3 PROBLEM STATEMENT

To analyze an high speed linear congruential generator using CNTFET technology ,by integrating power reduction techniques.

CHAPTER-3

AIM AND SCOPE OF THE PROJECT

3.1 OBJECTIVES

- To reduce the delay and area in the prefix computation stages within PG logic and bit-addition logic through the integration of novel techniques and methodologies.
- Aim to minimize the critical path, area delay product, and power-delay product by exploring advanced optimization techniques and circuit-level tuning strategies.
- Conduct a comparative analysis to evaluate the reduction in area utilization, timing path, and power dissipation between existing and proposed methodologies.
- Improve the performance of the MDCLCG architecture by implementing a three-operand adder and optimizing VLSI architecture for efficient three-operand binary addition.
- Conduct a thorough comparison of average power, delay, and product delay metrics to assess the effectiveness of proposed enhancements in improving overall system performance and efficiency.
- Assess the scalability of the proposed MDCLCG architecture to accommodate future technological advancements and scaling requirements, ensuring flexibility and adaptability to evolving performance and power efficiency challenges.
- Integration of Sleep Technique: Incorporating the sleep technique into the existing LCG system aims to reduce power consumption during idle states, thereby enhancing overall energy efficiency without compromising performance.
- Evaluation of Power-Delay Trade-offs: Conducting a comprehensive analysis to assess the trade-offs between power consumption and delay in both existing and proposed methodologies. This involves quantifying the impact of design choices on power-delay product and identifying optimal configurations that balance performance and energy efficiency.

- **Optimization of VLSI Architecture:** Developing an efficient VLSI architecture for fast three-operand binary addition entails optimizing hardware resources while meeting performance targets. This optimization may involve exploring novel circuit designs, layout strategies, or algorithmic enhancements to achieve the desired balance between speed, area, and power consumption.
- **Comparative Study of Performance Metrics:** Conducting a thorough comparison of average power, delay, and product delay between the existing and proposed methodologies. This comparative analysis provides insights into the effectiveness of the proposed enhancements in improving overall system performance and efficiency..

3.2 SCOPE OF THE PROJECT

In the future, various enhancements and improvements can be implemented to augment the existing system. This may involve integrating alternative methodologies and techniques to boost efficiency and effectiveness. Potential additions include exploring novel algorithms, circuit architectures, or optimization strategies to address identified limitations and optimize performance metrics.

Additionally, there is scope for designing and integrating new components, algorithms, or techniques into the existing system to improve functionality and performance. Through rigorous testing and evaluation, the impact of these enhancements on key performance metrics such as delay, area utilization, and power consumption can be quantified. Furthermore, assessing the scalability and applicability of proposed solutions across different scenarios or applications is essential, considering factors such as varying bit sizes, computational requirements, and resource constraints to ensure versatility and adaptability to diverse environments. Overall, future efforts will focus on a holistic approach to enhancing the efficiency, reliability, and scalability of the existing system through comprehensive analysis, innovative design, and rigorous evaluation.

CHAPTER-4

EXISTING SYSTEM

4.1 MDCLCG

The Modified Dual-CLCG (MDCLCG) emerges as a highly efficient method for generating Pseudo Random Bits (PRBG), especially suitable for hardware security applications based on stream ciphers. However, the robustness of the MDCLCG approach in terms of security is directly correlated with the bit size of the congruential modulus. Its unpredictability and security assurance are polynomial-time for $n \geq 32$ bits. The hardware architecture of MDCLCG is based on the Linear Congruential Generator (LCG), as depicted in the provided figure. The primary computational arithmetic block is a three-operand modulo- $2n$ adder. This architecture consists of four three-operand modulo- $2n$ carry-save adders (CS3A), two magnitude comparators, along with four registers and multiplexers. It's worth noting that the elongated carry propagation gate delay inherent in the CS3A adder significantly impacts the performance of the MDCLCG architecture, particularly as the bit size increases.

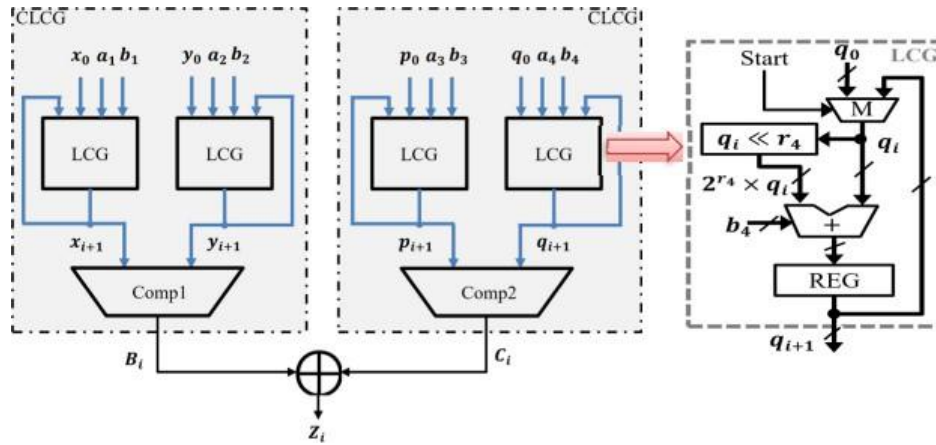


Fig 4.1 MDCLCG Architecture (Modified Dual Coupled Linear Congruential Generator)

In this section, the performance evaluation of MDCLCG delves into mitigating the effects of extended carry propagation delays by exploring alternatives to the CS3A adder. Specifically, we investigate the performance

metrics of MDCLCG architecture by replacing the CS3A adder with both HHC3A and proposed adder architectures. This comparative analysis aims to discern the impact of different adder designs on the overall performance of MDCLCG, considering factors such as throughput, area efficiency, and power consumption. By exploring alternative adder architectures, we seek to optimize the performance of MDCLCG, ensuring its efficacy and suitability for stream-cipher based hardware security applications across varying bit sizes of the congruential modulus.

4.2 LCG

The most popular method for producing random numbers is a technique known as the linear congruential generator. Lehmer presented the concept in accordance with the subsequent equation in

$$X_{n+1} = (aX_n + c) \bmod m \quad (1)$$

The modulus (m), multiplier(a) and increment (c) are crucial parameters in the configuration of a Linear Congruential Generator (LCG) that significantly affect its ability to produce a wide range of non-repeating values before reaching the modulus(m). The selection of these parameters must be done with precision to ensure the generation of a sequence of values that appears random and has a long period. According to the guidelines provided by Park and Miller, setting the increment (c) to 0 can yield any satisfactory results. In this setup, the multiplier(a) should be chosen from within the range of 2 to m-1, and the modulus (m) should be a large prime number. Although, the theoretical maximum cycle length of an LCG is the modulus (m), achieving this maximum length requires adherence to specific conditions.

- The increment (c) should be relatively prime to the modulus (m), ensuring that every possible value in the range can eventually be generated.
- The multiplier (a) minus 1 should be divisible by all prime factors of the modulus (m).

- When the modulus (m) is a multiple of 4, the multiplier (a) minus 1 should also be a multiple of 4. This condition helps in maintaining the cycle length by aligning the generator's operation with the modulus's properties.

Figure 4.2 illustrates a block diagram depicting the general operation of an LCG (Linear Congruential Generator), where the seed value is disregarded. The operation involves multiplication, addition, subtraction, and comparison blocks.

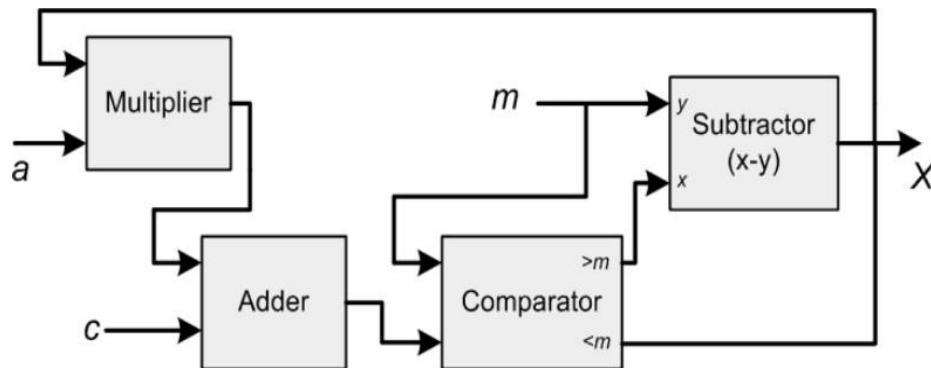


Fig 4.2 Block Diagram of LCG Operation

Initially, the multiplier multiplies the previous random value X by a , then adds the increment c . The resulting value is compared to the modulus m . If the number is less than or equal to m , it is considered a random number; otherwise, it is subtracted from m to obtain the random number. To streamline this process, the circuit is designed using word length reduction techniques as suggested. This design eliminates the need for the subtractor and comparator blocks, as depicted in Figure 4.2.1.

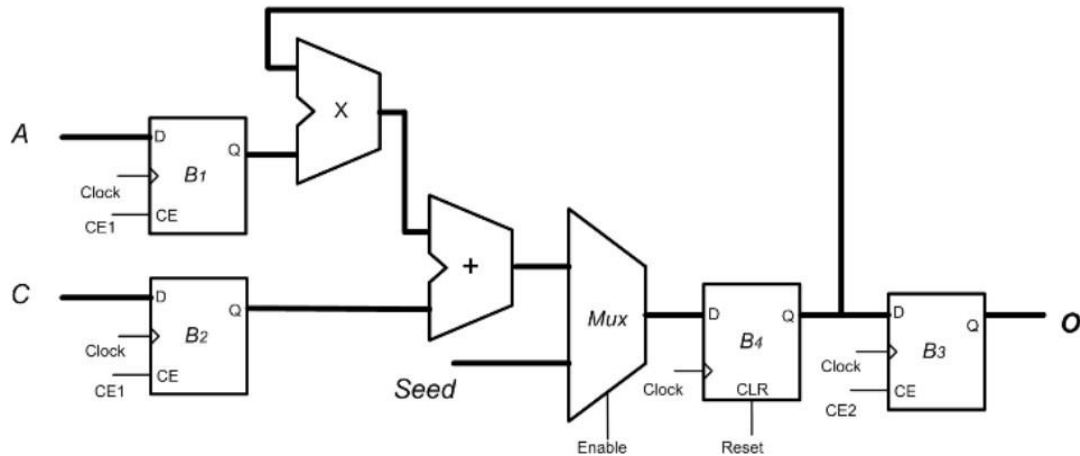


Fig 4.3 General Circuit Diagram Of LCG

When the “reset” signal is HIGH (and “enable” is LOW), the multiplexer selects the Seed value, which is then written into Buffer B4. This clears any previous values and sets the starting point for the random number generation. When the “enable” signal goes HIGH (and “reset” is LOW), the circuit starts generating random numbers. With each clock pulse the previous random number from Buffer B4 is fed into B1. With each clock pulse the previous random number from Buffer B4 is fed into Buffer B1. The selected value is multiplied by A and stored in Buffer B2. The value in B2 is added to C and stored in Buffer B3.

Instead of comparing B3 with the modulus (m), the adder wraps around if the sum exceeds m. This means it automatically subtracts m from the sum, effectively achieving the comparison and subtraction in one step. The final random number (now within the range) is written to Buffer B4, overwriting the previous one. This process repeats with each clock cycle, generating a new random number based on the previous one. The sequence depends on the initial seed, A, and C values. The LCG circuit is analysed using the 130nm and 32 nm MOSFET and 32nm CNTFET technology.

Advantages of LCG:

1. LCGs are known for their speed and efficiency, requiring minimal memory to retain state.
2. CLCG provides a streamlined and efficient approach to generating pseudo-random numbers.

3. LCG algorithm implementation is cost-effective and does not require extensive resources.

Disadvantages of LCG:

1. LCGs are unsuitable and should not be used for cryptographic applications due to their inherent weaknesses.
2. Sequential correlation on successive calls can compromise the randomness of LCG-generated numbers, limiting their reliability in certain contexts.

4.3 CNTFET TECHNOLOGY

Carbon Nanotube Field-Effect Transistor (CNTFET) technology is an innovative semiconductor technology that uses carbon nanotubes (CNTs) as the channel material instead of traditional silicon in the transistor design. Carbon nanotubes are cylindrical molecules made of carbon atoms arranged in a hexagonal lattice, resembling rolled-up sheets of graphene. These nanotubes exhibit remarkable electrical, thermal, and mechanical properties, making them highly attractive for electronic device applications. CNTFETs operate on the same principle as conventional silicon-based Field-Effect Transistors (FETs), where a gate voltage controls the flow of electrical current between the source and drain terminals through a channel. However, the use of CNTs as the channel material in CNTFETs offers several potential advantages over silicon, including higher electron mobility, greater current density, and the possibility of ballistic transport, where electrons move through the channel with minimal scattering, thus reducing power consumption and improving device performance.

The promise of CNTFET technology lies in its potential to enable the continued miniaturization of electronic components while overcoming some of the physical limitations faced by silicon-based devices, especially as the industry approaches the limits of Moore's Law. CNTFETs could lead to the development of faster, more energy-efficient electronic devices, ranging from processors and memory to sensors and flexible electronics.

4.3.1 DEVICE PARAMETERS OF CNTFET

In the detailed analysis of Carbon Nanotube Field-Effect Transistors (CNTFETs), several device parameters play pivotal roles in dictating the performance and applicability of these advanced semiconductor devices. A critical aspect of CNTFETs is their reliance on the unique properties of carbon nanotubes (CNTs), which serve as the conductive channel between the transistor's source and drain. The chirality of the CNT, denoted as (n, m) , is fundamental in determining the electrical behaviour of the CNT, categorizing it as either metallic or semiconducting. This distinction is vital for the design of CNTFETs, as semiconducting CNTs are preferred for transistor applications due to their ability to switch between conducting and insulating states. The diameter of the CNT, denoted as d_{CNT} , is another crucial parameter that influences the device's electrical characteristics, including the threshold voltage and current.

The diameter, which is intrinsically linked to the CNT's chirality, also affects the bandgap of the CNT, thus impacting the device's performance in semiconductor applications. Typically, d_{CNT} values are in the range of 1-2 nm, aligning with the need for semiconducting behaviour in CNTFETs. Gate length (L_g) is paramount in controlling the short-channel effects that are critical when scaling down devices for high-density applications. Similar to traditional silicon-based FETs, the gate length in CNTFETs influences the electrostatic control over the channel, with shorter gate lengths generally leading to enhanced device performance but at the risk of exacerbated short-channel effects.

The gate oxide thickness (t_{ox}) directly impacts the gate capacitance and, consequently, the switching speed of the device. A thinner gate oxide is beneficial for achieving higher drive currents due to the stronger capacitive coupling between the gate and the channel. However, this advantage comes at the cost of increased gate leakage, posing a design challenge. Gate oxides are often made of high-k materials to mitigate these issues, with thicknesses typically around 1-2 nm. Channel length (L_{ch}), the distance between the source and drain contacts along the CNT, is a defining feature of CNTFETs that affects their operational speed. Reducing the channel length can potentially improve the device's speed by

shortening the path electrons must travel. However, very short channel lengths may introduce undesirable short-channel effects, demanding careful optimization of this parameter. Lastly, the source/drain contact resistance (R_{sd}) is a significant factor affecting the overall performance of CNTFETs.

Table 4.1 Device Parameters Of CNTFET

Device Parameter	Values
Chirality of tube	(19,0)
CNT diameter	0.7 nm-2 nm
Gate length	32 nm
Gate oxide thickness	1 nm- 2nm
Channel Length	32 nm

4.3.2 DEVICE PERFORMANCE OF CNTFET

CNTFETs harness the unique properties of carbon nanotubes (CNTs) to achieve superior performance, which is characterized by several key factors. Like traditional Field-Effect Transistors (FETs), CNTFETs control the flow of current through a semiconductor channel with an electric field introduced by a gate electrode. The semiconductor in this case is a carbon nanotube, which can be either a single-walled carbon nanotube (SWCNT) or a multi-walled carbon nanotube (MWCNT), depending on the design. The source and drain contacts are made on either end of the CNT, and the gate electrode can be placed either below the CNT (as in a back-gated configuration) or surrounding it (in a top-gated configuration).

The gate electrode is separated from the CNT by a thin insulating layer known as the gate dielectric. Applying a voltage to the gate electrode creates an electric field across the dielectric, and influencing the energy bands of the CNT and thereby controlling the flow of the electrons between the source and drain contacts. For n-type operation, applying a positive gate voltage attracts electrons into the CNT, lowering the energy barrier for electron transport and allowing current to flow. Conversely, when the gate voltage is removed or made negative,

the energy barrier increases, preventing electron flow and turning the device off. The operation is similar but with opposite polarities for p-type CNTFETs. The quantum mechanical properties of CNTs play a crucial role in their operation as transistors. The bandgap of a CNT — the energy difference between its valence and conduction bands — determines its electrical conductivity and is directly influenced by the nanotube's diameter and chirality. This bandgap gives CNTFETs their semiconducting properties and allows for the fine-tuning of device characteristics by selecting CNTs with specific physical properties. Electron transport in CNTs is also significantly affected by quantum confinement, as electrons in the quasi-one-dimensional structure of a CNT behave as quantum waves. This confinement leads to discrete energy levels within the CNT and allows for ballistic transport of electrons, where they can travel through the CNT without scattering, under certain conditions.

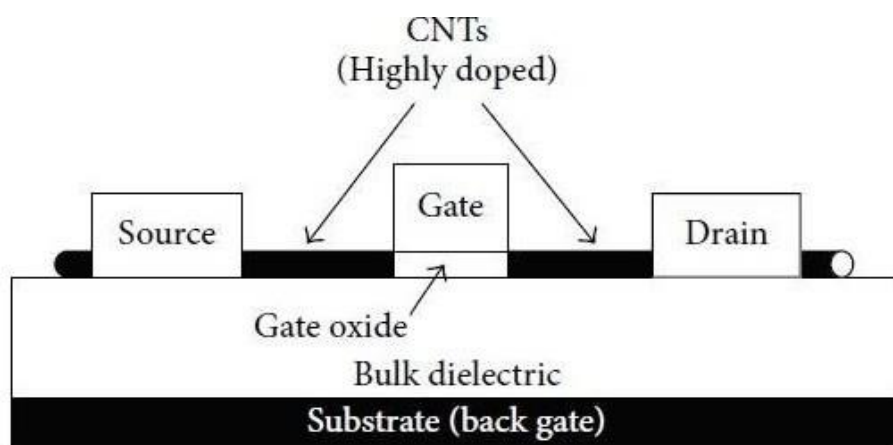


Fig 4.4 CNTFET Diagram

CHAPTER-5

PROPOSED SYSTEM

5.1 SLEEP TECHNIQUE FOR LEAKAGE POWER REDUCTION IN LCG

The sleep technique is a cutting-edge solution designed to tackle the issue of leakage power in digital circuits, a significant concern as technology continues to scale down. This method is particularly beneficial in applications requiring constant operation, like Linear Congruential Generators (LCGs), where power efficiency is critical. At the heart of the sleep technique lies its unique approach to managing power at the component level. The strategy involves the use of two transistors: a PMOS transistor connected to the positive power supply (VDD) and an NMOS transistor connected to the ground.

These transistors act as switches that control the flow of power to the circuit's components. In periods of inactivity, the PMOS transistor is turned off, cutting off the power supply, while the NMOS transistor is turned on, connecting the component to the ground. This state significantly reduces the leakage current, which is a primary source of power wastage in idle digital circuits. The operational principle of the sleep technique is based on dynamically toggling the state of the circuit components between active and sleep modes, depending on their usage. In the sleep mode, by disconnecting the components from VDD and grounding them, the technique effectively minimizes the leakage current.

This is crucial for maintaining energy efficiency, especially in devices where the components are not always needed but cannot be completely powered down due to system requirements. Implementing the sleep technique across our project's key components, including D Flip-Flops (DFFs), multiplexers (MUX), and AND/OR gates, was a strategic move to combat leakage power, crucial for enhancing the energy efficiency of our Linear Congruential Generator (LCG) system. This was achieved by adding a PMOS transistor connected to the power supply (VDD) and an NMOS transistor connected to the ground for each component.

These transistors serve as switches that control the power flow: when a component is idle, the PMOS transistor is turned off to cut the power supply, and the NMOS transistor is turned on to ground the component, significantly reducing leakage power. In practice, this meant integrating the sleep technique at the circuit level, ensuring each DFF, MUX, and logic gate could enter a low-power state without affecting the system's functionality. For DFFs, which are crucial for timing and data storage, implementing sleep mode ensured they only consumed power when updating or holding data. For MUX'es, which direct data paths in the LCG, and AND/OR gates, crucial for logical operations, the sleep technique minimized power usage when their operations were not required, thereby reducing overall energy consumption without compromising the accuracy or speed of the pseudorandom number generation. This approach not only showcased our project's commitment to energy efficiency but also demonstrated the practicality of the sleep technique in reducing leakage power across various digital components, ensuring our LCG system remains both effective and environmentally conscious.

CHAPTER-6

RESULTS AND DISCUSSION

6.1 SIMULATION RESULT OF EXISTING SYSTEM

The power consumption, delay, and Power-Delay Product (PDP) were observed to decrease in the CNTFET 32 nm technology utilizing when compared to 32 nm and 130 nm MOSFET technology. Further reductions in power, delay, and PDP were achieved in the proposed system, by modifying the existing system with leakage power reduction technique to Carbon Nanotube Field-Effect Transistor (CNTFET) technology. The below figure shows the output waveforms of LCG using 130nm MOSFET technology and 32nm CNTFET and MOSFET technology.

The below table presents a comprehensive performance analysis of Linear Congruential Generators (LCG) utilizing MOSFET at both 32 nm and 130 nm technology, and Carbon Nanotube Field-Effect Transistors (CNTFET) at the 32 nm technology. This analysis covers critical performance metrics such as power consumption, delay, and Power Delay Product (PDP), across several key digital components: adders, D Flip-Flops (DFF), multiplexers (MUX), and the LCG itself. Through this detailed examination, comparisons are drawn to highlight the efficiency and effectiveness of the existing system across different configurations and technology.

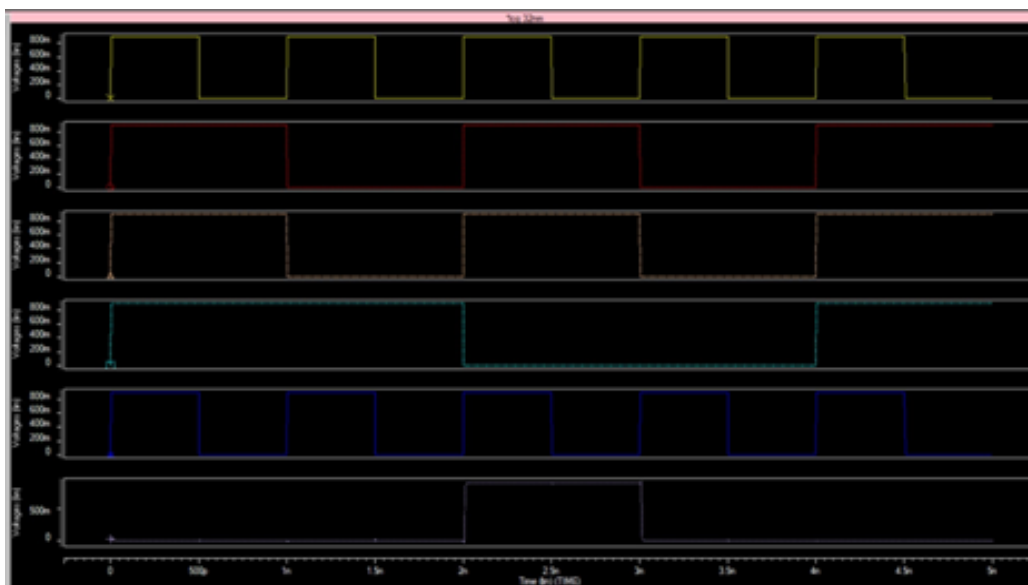


Fig 6.1 LCG in 130nm MOSFET Technology

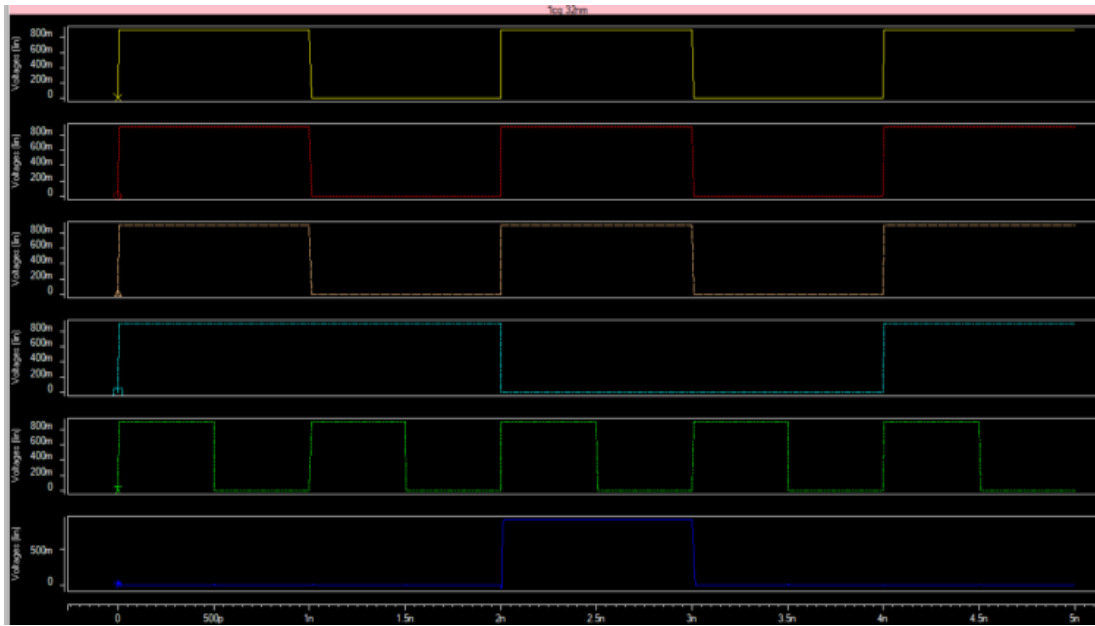


Fig 6.2 LCG in 32nm MOSFET Technology

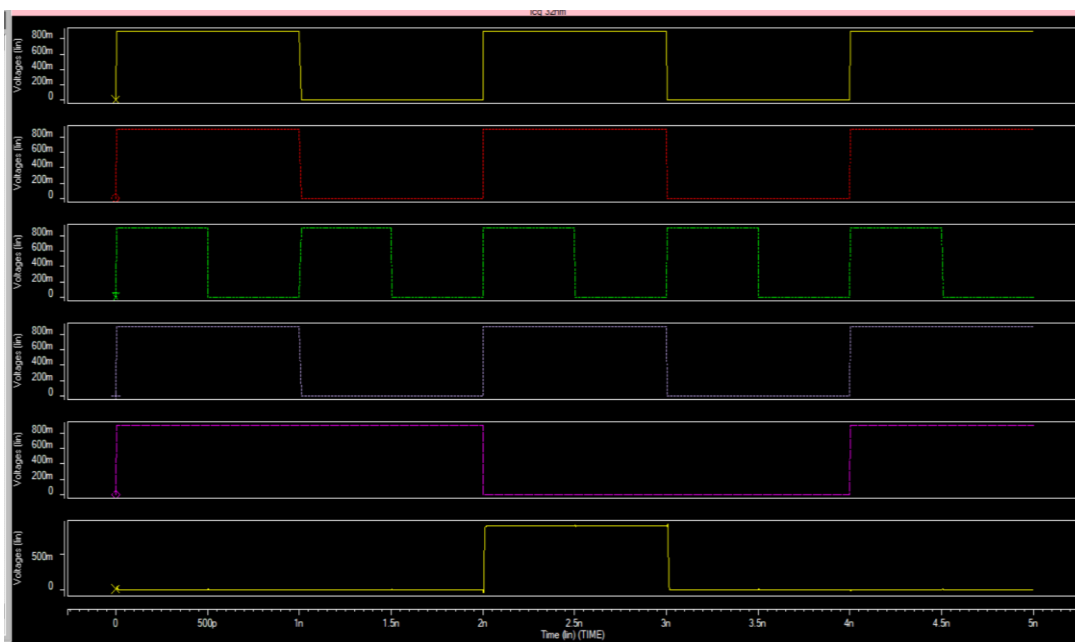


Fig 6.3 LCG in 32nm CNTFET Technology

Table 6.1 Comparison analysis of LCG under 130nm ,32nm MOSFET and 32nm CNTFET

DEVICE	130nm MOSFET		
	Power(W)	Delay(s)	PDP(J)
ADDER	1.715×10^{-5}	270.99P (10^{-12})	4.6474F(10^{-15})
AND	1.790×10^{-5}	46.594 P	0.8340 F
DFF	4.432×10^{-5}	36.998 P	1.6397 F
MUX	1.752×10^{-5}	1.113 P	0.0195 F
LCG	2.096×10^{-4}	11.93 P	2.5005 F

32nm MOSFET		
Power(W)	Delay(s)	PDP(J)
1.697×10^{-7}	2.417 P(10^{-12})	0.4103 A(10^{-18})
1.962×10^{-7}	4.6525 P	0.9123 A
0.480×10^{-6}	6.1072 P	2.9351 A
8.33×10^{-6}	152.36 P	1269615 A
2.058×10^{-5}	8.7748 P	180.58 A

DEVICE	32nm CNTFET		
	Power(W)	Delay(s)	PDP(J)
ADDER	9.471×10^{-8}	498.85P(10^{-12})	47.246A(10^{-18})
AND	7.632×10^{-8}	57.543 F	0.00439 A
DFF	2.315×10^{-20}	57.024 F	0.00132 A
MUX	6.976×10^{-8}	27.578F	0.00192 A
LCG	2.848×10^{-21}	372.73 F	0.01061 A

6.2 SIMULATION RESULTS AND COMPARITIVE ANALYSIS OF PROPOSED SYSTEM

After implementing the sleep technique aimed at reducing leakage power, our comparative simulation study underscored the efficacy of this approach across various digital components within Linear Congruential Generator (LCG) systems. Utilizing 32 nm Carbon Nanotube Field-Effect Transistor (CNTFET) technology, we observed a marked enhancement in performance over the conventional 130 nm and 32 nm MOSFET technology. This improvement was consistently evident in digital components such as adders, AND gates, D Flip-Flops (DFF), multiplexers (MUX), and the LCG itself, where key metrics like power consumption, delay, and Power Delay Product (PDP) saw significant advancements. The simulation results, alongside detailed tables, comprehensively illustrate the beneficial impact of incorporating sleep techniques with CNTFET technology, highlighting its potential in advancing the energy efficiency of LCG systems and potentially other digital circuits.

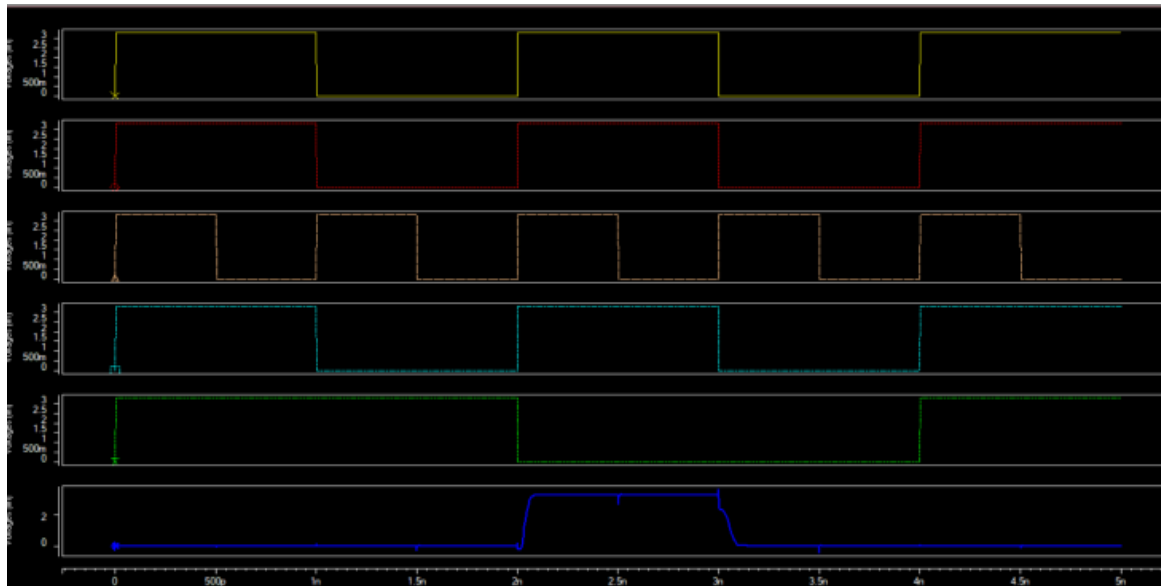


Fig 6.4 LCG with sleep technique in 130 nm MOSFET

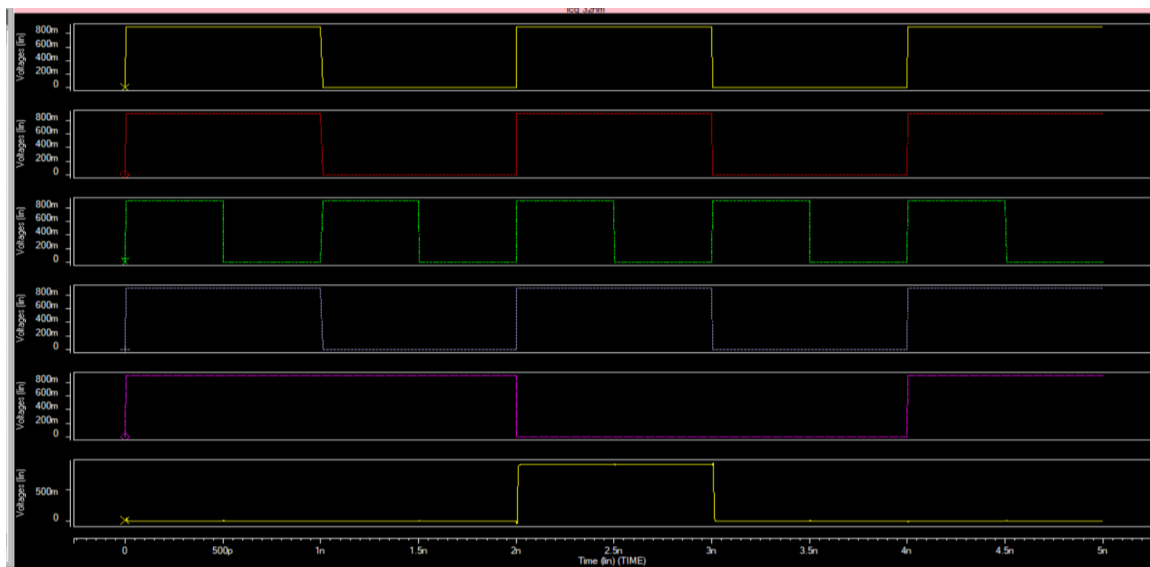


Fig 6.5 LCG with sleep technique in 32 nm MOSFET

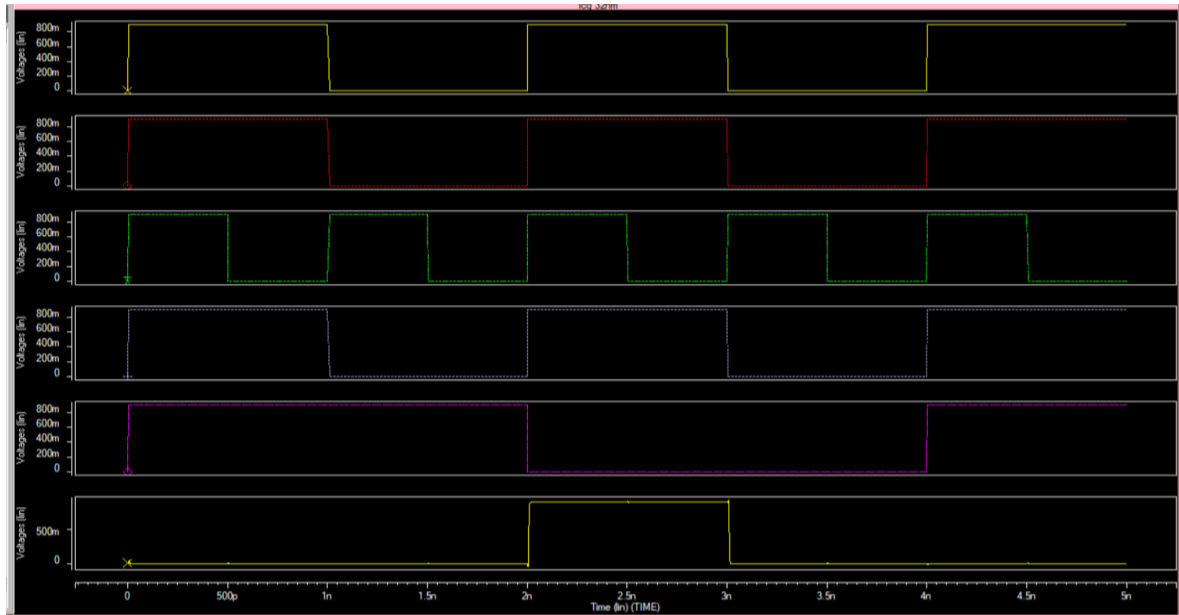


Fig 6.6 LCG with sleep technique in 32 nm CNTFET

Table 6.2 Comparison analysis of LCG with sleep technique under 130 nm MOSFET ,32 nm MOSFET and 32 nm CNTFET

DEVICE	130nm MOSFET		
	Power(W)	Delay(s)	PDP(J)
ADDER	1.715×10^{-5}	270.99P (10^{-12})	4.6474F(10^{-15})
AND	1.790×10^{-5}	46.594 P	0.8340 F
DFF	4.432×10^{-5}	36.998 P	1.6397 F
MUX	1.752×10^{-5}	1.113 P	0.0195 F
LCG	2.096×10^{-4}	11.93 P	2.5005 F
LCG with sleep	2.226×10^{-4}	39.27 P	0.0874 F

32nm MOSFET		
Power(W)	Delay(s)	PDP(J)
1.697×10^{-7}	$2.417 \text{ P}(10^{-12})$	$0.4103 \text{ A}(10^{-18})$
1.962×10^{-7}	4.6525 P	0.9123 A
0.480×10^{-6}	6.1072 P	2.9351 A
8.33×10^{-6}	152.36 P	1269615 A
2.058×10^{-5}	8.7748 P	180.58 A
2.088×10^{-5}	5.569 P	0.0162 F

DEVICE	32nm CNTFET		
	Power(W)	Delay(s)	PDP(J)
ADDER	9.471×10^{-8}	$498.85 \text{ P}(10^{-12})$	$47.246 \text{ A}(10^{-18})$
AND	7.632×10^{-8}	57.543 F	0.00439 A
DFF	2.315×10^{-20}	57.024 F	0.00132 A
MUX	6.976×10^{-8}	27.578 F	0.00192 A
LCG	8.091×10^{-17}	235.83 F	0.01908 A
LCG with sleep	2.144×10^{-6}	575.79 F	1.234 A

CHAPTER – 7

CONCLUSION

7.1 CONCLUSION

The utilization of sleep techniques for leakage power reduction within Linear Congruential Generators (LCG), utilizing 32 nm Carbon Nanotube Field-Effect Transistor (CNTFET) technology, signifies a notable leap forward compared to conventional 130 nm MOSFET methodologies. Extensive comparative simulations have underscored the significant enhancements in power efficiency achievable through the integration of CNTFET technology alongside sleep techniques. Evident from these simulations are marked reductions in power consumption, delay, and optimized Power Delay Product (PDP) observed across various digital components.

These compelling results not only underscore the potential of CNTFET technology to augment energy efficiency but also herald a promising trajectory for future investigations in digital circuit optimization. By shedding light on the effectiveness of innovative approaches in semiconductor technology, this project underscores the crucial role of research and development in advancing sustainable electronic devices.

In conclusion, this project's findings contribute valuable insights into the realm of electronic device development, emphasizing the significance of adopting novel methodologies such as sleep techniques in conjunction with advanced semiconductor technologies like CNTFET. By showcasing substantial improvements in power efficiency and performance metrics, the study underscores the potential of innovative approaches to drive advancements in digital circuit optimization. Moving forward, the project's conclusions advocate for continued exploration and refinement of such techniques to realize more sustainable and energy-efficient electronic devices, thereby furthering the evolution of semiconductor technology towards a greener and more efficient future.

7.2 STANDARDS

Adherence to industry standards serves as a cornerstone of our project, ensuring that our methodologies and findings meet recognized benchmarks within the semiconductor technology domain. Embracing established guidelines such as IEEE standards for digital circuit design, we have adopted robust practices endorsed by industry experts. By aligning with these standards, we assure the reliability and quality of our work, adhering to rigorous criteria for performance, efficiency, and compliance. Moreover, our commitment to ISO standards for energy efficiency underscores our dedication to sustainability, as we strive to develop electronic devices that not only meet functional requirements but also adhere to stringent energy consumption guidelines. Incorporating these standards into our project framework underscores our commitment to excellence and professionalism in semiconductor research and development.

In the pursuit of excellence, our project upholds the principles of industry standards, ensuring that our methodologies and outcomes meet established benchmarks and specifications. By adhering to respected guidelines such as IEEE standards for digital circuit design, we embrace best practices endorsed by the industry, fostering reliability and consistency in our approach. This adherence to standards not only enhances the credibility of our work but also facilitates interoperability and collaboration within the broader semiconductor community. Additionally, our alignment with ISO standards for energy efficiency underscores our dedication to sustainable technology, as we strive to minimize environmental impact and promote energy-conscious design practices. By integrating these standards into our project framework, we reaffirm our commitment to innovation, quality, and responsible technology development.

7.3 CONSTRAINTS

Throughout our project journey, we encountered various constraints that shaped our decisions and influenced project outcomes. One significant constraint was the limitation of hardware resources available for experimentation and testing, necessitating careful resource management and optimization strategies.

Furthermore, time constraints imposed tight deadlines for project milestones, requiring efficient planning and prioritization to meet project objectives within schedule. Additionally, budget constraints posed challenges in resource allocation, influencing decisions regarding equipment procurement and research activities. Despite these constraints, we navigated challenges adeptly, devising innovative solutions and strategies to mitigate their impact and ensure successful project execution.

The realization of our project goals was punctuated by a series of constraints that demanded creative problem-solving and strategic decision-making. Notably, the scarcity of hardware resources posed challenges in conducting experiments and simulations, prompting us to devise efficient resource allocation strategies and prioritize essential tasks. Moreover, time constraints-imposed pressures to meet project deadlines, necessitating careful planning and execution to ensure timely delivery of project milestones. Additionally, budget limitations influenced resource allocation decisions, requiring judicious spending and cost-effective solutions. Despite these constraints, our project thrived on resilience and adaptability, as we leveraged ingenuity and collaboration to overcome obstacles and achieve success.

REFERENCES

1. Barkhordarian, Vrej. "Power MOSFET basics." Power conversion and Intelligent Motion-English Edition 22, no. 6 (1996): 2-8.
https://caxapa.ru/thumbs/804043/mosfet_basic.pdf
2. Gadgil, Sharvani, and Chetan Vudadha. "Design of CNTFET-based ternary ALU using 2: 1 multiplexer based approach." IEEE Transactions on Nanotechnology 19 (2020): pp. 661-671.
<https://ieeexplore.ieee.org/abstract/document/9174868>
3. Gavaber, M. Dadashi, K. Manochehri Kalantari, and Saadat Pourmozafari. "Design of high speed and low power D Flip-Flop by CNTFET technology." In 3rd International Conference on Knowledge-Based Engineering and Innovation, Tehran, Iran. 2016.
<https://n9.cl/m0vas>
4. Hartmann, Martin, Sascha Hermann, Phil F. Marsh, Christopher Rutherglen, Dawei Wang, Li Ding, Lian-Mao Peng, Martin Claus, and Michael Schröter. "CNTFET technology for RF applications: Review and future perspective." IEEE Journal of Microwaves 1, no. 1 (2021): 275-287.
<https://ieeexplore.ieee.org/abstract/document/9318747>
5. Khan, Imtiyaz Ahmad, and Naushad Alam. "CNTFET based circuit design for improved performance." In 2019 International Conference on Electrical, Electronics and Computer Engineering (UPCON), pp. 1-5. IEEE, 2019.
https://ieeexplore.ieee.org/abstract/document/8980053?casa_token=zI2n4RMJsSYAAAAA:Fn5PZAw0HDwqnb3N0xqteSki2HeqBBstX9dLWYYw2a6d_KyLhjmtFSzs0hgqYtHtr_UOHMvdg-nPBQ
6. Kim, Kyung Ki, Haiqing Nan, and Ken Choi. "Hybrid MOSFET/CNFET based power gating structure." In 23rd IEEE International SOC Conference, pp. 334-338. IEEE, 2010.
https://ieeexplore.ieee.org/abstract/document/5784689?casa_token=Ue8wV3AW4jUAAAAA:EApVG9bJoZ7uxb7pzRK7vHH6fQaOIXbB7C3tLs5DI7HE8lrpZMSjWcC5ixMblRZEYlQnlAzFlzIRPg
7. Krawczyk, Hugo. "How to predict congruential generators." In Conference on the Theory and Application of Cryptology, pp. 138-153. New York, NY: Springer New York, 1989.
https://link.springer.com/chapter/10.1007/0-387-34805-0_14
8. Kumar Panda and K. Chandra Ray, "A coupled variable input LCG method and its VLSI architecture for pseudorandom bit generation", IEEE Trans. Instrum. Meas., vol. 69, no. 4, pp. 1011-1019, Apr. 2020.
https://scholar.google.com/scholar?as_q=A+coupled+variable+input+LCG+method+and+its+VLSI+architecture+for+pseudorandom+bit+generation&as_occt=title&hl=en&as_sdt=0%2C31

9. L'Ecuyer, Pierre, and François Blouin. "Linear congruential generators of order $k > 1$." In 1988 Winter Simulation Conference Proceedings, pp. 432-439. IEEE, 1988.
<https://ieeexplore.ieee.org/abstract/document/716197>
10. Marsaglia, George. "The structure of linear congruential sequences." In Applications of number theory to numerical analysis, pp. 249-285. Academic Press, 1972.
<https://www.sciencedirect.com/science/article/abs/pii/B9780127759500500133>
11. O'Connor, Ian, Junchen Liu, Frédéric Gaffiot, Fabien Prégaldiny, Christophe Lallement, Cristell Maneux, Johnny Goguet et al. "CNTFET modeling and reconfigurable logic-circuit design." IEEE Transactions on Circuits and Systems I: Regular Papers 54, no. 11 (2007): 2365-2379.
<https://ieeexplore.ieee.org/abstract/document/4383253>
12. Peng, B., Annamalai, M., Mothes, S. et al. Device design and optimization of CNTFETs for high-frequency applications. J Comput Electron 20, 2492–2500 (2021).
<https://doi.org/10.1007/s10825-021-01805-5>
13. Polat, Övünç, and Ali Manzak. "Design and analysis of low power Carbon Nanotube Field Effect Transistor (CNFET) D Flip-Flops (DFFs)." In 2011 3rd International Conference on Computer Research and Development, vol. 3, pp. 399-401. IEEE, 2011.
https://ieeexplore.ieee.org/abstract/document/5764223?casa_token=qp6khGFVRZsAAAAA:cGEAuW5pdQwxMgL7sRr3eiwrRRyRjkh4JqE1ZjuWu6vJsNP NJuAgM63LMiU7YNXqnf-_zh2pC2N27A
14. Prasad, S. Rajendra, B. K. Madhavi, and K. Lal Kishore. "Reduction of leakage-power in CNTFET SRAM cell using stacked sleep technique at 32nm technology." In IEEE-International Conference On Advances In Engineering, Science And Management (ICAESM-2012), pp. 233-237. IEEE, 2012.
https://ieeexplore.ieee.org/abstract/document/6216005?casa_token=O8dbJ4iHI-4AAAAA:09Q4PfQFXJlgMdjExuelwl97tee2zYuS__ZgXQ68bjYFbVgtKqE0cd hcoxYPWe79mBQOJ624djreJQ
15. Ravi, T., and V. Kannan. "Design and analysis of N-type CNTFET based double edge triggered D flip-flop." Nation. J. Elect. Sci. Syst. 2 (2011):pp. 53-59.
<https://www.proquest.com/openview/bba2a1fa64a1c1c7c5a44f930bfab379/1?pq-origsite=gscholar&cbl=2041018>
16. Sathyakala, Ms D., Ms M. Mathumat, Ms T. DHEIVA Priya, and Ms S. Deepika. "An efficient fir filter design using three-operand binary adder." Int

Res J Eng Technol 8, no. 3 (2021):pp. 3166-3171.
<https://n9.cl/pu8ys>

17. Sahai, Avichal, and Vikas Sharma. "Design of low power CNTFET based D flip flop using sleep transistor technique." International Journal of Engineering Research & Technology (IJERT) 4, no. 4 (2015):pp. 541-545.
<https://n9.cl/ukmvw>
18. Shanmugam, K., Kumar, C., Fayek, H. H., & Rusu, E. (2023). "Design and Implementation of CNFET SRAM Cells by Using Multi-Threshold Technique." Electronics, 12(7), 16111
<https://doi.org/10.3390/electronics12071611>
19. Sridharan, K., Sundaraiah Gurindagunta, and Vikramkumar Pudi. "Efficient multiterinary digit adder design in CNTFET technology." IEEE transactions on Nanotechnology 12, no. 3 (2013):pp. 283-287.
<https://ieeexplore.ieee.org/abstract/document/6475189>
20. Sujitha, A., L. Lakshmi, N. Mathan, and R. Narmadha. "Analysis of an Efficient Linear Congruential Generator Architecture for Digital Applications." In 2023 Fifth International Conference on Electrical, Computer and Communication Technologies (ICECCT), pp. 1-4. IEEE, 2023.
<https://ieeexplore.ieee.org/abstract/document/10179609>
21. Sushmitha, M., K. Jamal, M. Kiran, OVP Kumar Manchalla, and Ch Pratyusha Chowdari. "MDCLCG with Square Root Carry Select Adder Technique for Hardware Security." In 2022 International Conference on Augmented Intelligence and Sustainable Systems (ICAISS), pp. 916-924. IEEE, 2022.
https://ieeexplore.ieee.org/abstract/document/10010741?casa_token=OI839ntMM1gAAAAA:EnMN6ZO1eZMtBqdKC9uoFaJWRhvpj7qwVGARA2wjY_TP6_8dHulGUKL5rd2jpsCIS9UgFCyBwuRi-A
22. Suvvari, Shyam Kumar, and AS Srinivasa Rao. "AREA EFFICIENT DESIGN OF THREE OPERAND BINARY ADDER FOR CRYPTOGRAPHIC APPLICATIONS."
<https://advancedengineeringsscience.com/article/pdf/2023/02-323.pdf>
23. Tezuka, Shu. "Linear congruential generators." In Uniform Random Numbers: Theory and Practice, pp. 57-82. Boston, MA: Springer US, 1995.pp.323-328.
https://link.springer.com/chapter/10.1007/978-1-4615-2317-8_3
24. Westlake, Wilfred J. "A uniform random number generator based on the combination of two congruential generators." Journal of the ACM (JACM) 14, no.2 (1967):pp. 337-340.
<https://dl.acm.org/doi/abs/10.1145/321386.321396>