Indonesian Journal of Electrical Engineering and Informatics (IJEEI)
Vol. 7, No. 4, Dec 2019, pp. 697~702
ISSN: 2089-3272, DOI: 10.11591/ijeei.v7i4.1459

Performance Analysis of Montgomery Multiplier using 32nm CNTFET Technology

Mathan N[1], Jayashri S[2], Nurul Ezaila Alias[3], Michael Loong Peng Tan[4]
[1]Faculty of Electronics Engineering, Sathyabama Institute of Science and Technology, Chennai, India
[2]Department of ECE, Adhiparasakthi Engineering College, Melmaruvathur, India
[3,4]School of Electrical Engineering, Faculty of Engineering, UniversitiTeknologi Malaysia, 81310, Johor, Malaysia

Article Info

Article history:

Received Sep 30, 2019
Revised Oct 18, 2019
Accepted Jan 02, 2020

Keyword:

Montgomery multiplier
Carbon Nanotube
Field ffect transistor
Power Delay Product

ABSTRACT

VLSI design vacillating the parameters results in variation of critical factors like area, power and delay. The dominant sources of power dissipation in digital systems are the digital multipliers. A digital multiplier plays a major role in a mixture of arithmetic operations in digital signal processing applications hinge on add and shift algorithms. In order to accomplish high execution speed, parallel array multipliers are comprehensively put into application. The crucial drawback of these multipliers is that it exhausts more power than any other multiplier architectures. Montgomery Multiplication is the popularly used algorithm as it is the most efficient technique to perform arithmetic based calculations. A high-speed multiplier is greatly coveted for its extraordinary leverage. The primary blocks of a multiplier are basically comprised of adders. Thus, in order to attain a significant reduction in power consumption at the chip level the power utilization in adders can be decreased. To obtain desired results in performance parameters of the multiplier an efficient and dynamic adder is proposed and incorporated in the Montgomery multiplier. The Carbon Nanotube field effect transistor (CNTFET) is a promising new device that may supersede some of the fundamental limitations of a silicon based MOSFET. The architecture has been designed in 130nm and 32nm CMOS and CNTFET technology in Synopsys HSpice. The analysed parameters that are considered in determining the performance are power delay product, power and delay and comparison is made with both the technologies.The simulation results of this paper affirmed the CNTFET based Montgomery multiplier improved powerconsumption by 76.47%,speed by 72.67% and overall energy by 67.76% as compared to MOSFET-based Montgomery multiplier.

Corresponding Author:

Mathan N,
Faculty of Electronics Engineering,
Sathyabama Institute of Science and Technology,
Chennai, India.
Email: mathanmaestro@hotmail.com

1. INTRODUCTION

In VLSI design, any modification in the architecture may bring changes in major factors like power, area and speed. A multiplier has a major role in a mixture of arithmetic operations in digital processing applications.The increase in operating frequency, semiconductor technology and chip density has resulted in increased use of power in VLSI circuits, which has become a major problem. A fast growing technology put forth demands for high- speed and efficient real time digital applications [1]. Silicon based technology might probably get reduced by 2020 as the length of the channel in a MOSFET can be less than 10nm. As the silicon

based devices face the scaling disadvantage the semiconductor industry is in search for devices and materials [2] that can be incorporated into the contemporary silicon-based technology in the future for a long term [3]. The count of analysing substitute results is single-electron tunnelling, rapid single-flux quantum logic, quantum cellular automata and Carbon Nanotube (CNT). After several experimental analyses, Carbon Nanotube has been found as the most promising alternate material.The diameter of CNT is found to be between 1 to 3 nm and its length extending to a few microns. CNTFETs can be used to a high extent for building both high-strength interconnections and low resistance [4].CNTs can be exploited to build both low-resistance, high-strength interconnections and highly scalable low-power carbon Nanotube field-effect transistors (CNTFET) and single electron tunnelling transistors are one of the basic ideas to replace the silicon MOSFETs with CNTFETs to overcome all the demerits of silicon MOSFETs. The highly scalable low-power Carbon Nanotube field-effect transistors (CNTFET) and single electron tunnelling transistors are quite few among the primary ideas to take over the MOSFETs (Silicon based) with CNTFET in order to surmount the constraints of the former. With the circuit design established on aforementioned devices will require the accessible device models and must be adaptable to the current flow of designs.

The paper is systematized as: In section II the geometrical structure of the carbonanotube field effect transistor (CNTFET) is briefly presented. Section III depicts Proposed Full adder cell and Montgomery Multiplier, Section IV illustrates Performance Analsyis by comparing both MOSFET and CNTFET technology, Conclusion and possible future oversight are inspected in section V.

2. CARBON NANO TUBE FIELD EFFECT TRANSISTOR

The term CNTFET is abbreviated as Carbon Nanotube Field Effect Transistor and it cites to a FET that resorts to single walled Carbon Nanotube or an assortment of carbon nanotube as the material used for channel instead of the silicon that has been used in the typical structure of MOSFET. During 1998, it was first manifested, that there are major developments in CNTFETs that vow to replace silicon in future electronics as an alternative material. Three presumptions are highly essential to presume that a CNTFET is prevailing in the region of ballistic. Carrier scattering events is quasi-suppressed in the intrinsic channel or channel carriers are scatter-free and all carriers propagating to the drain reach the drain without scattering back to the source. In this case, the carrier's transport is ballistic and in the ohmic zone, the drain current is expressed without depending on the carrier mobility with elementary parameters. This current is proportional to the channel width or nanotube diameter depending on the channel length [5]. The bread of Carbon Nanotube is characterized by capacitors of four different types, namelydrain,source, substrate and gate. The capacitance at gate terminal is reasonably higher than the three others (particularly when using high-k gate dielectrics) capacitors. The total capacitance apexes the quantum capacitance. CNTFETs functions in quantum capacitance limit. The charge at the inception of the channel is almost autonomous of the drain voltage when the gate capacitance is greater than quantum. Semiconducting CNTs were used to fabricate CNTFETs that show promise over silicon based MOSFETs due to their superior electrical characteristics[6][7].

When a gate capacitance is greater than the quantum capacitance, the charge at the beginning of the channel decreases when drain capacitance increases. The Figure 1 depicts the typical CNTFET device[6]. The 2D electrostatics, parasitic resistance and scattering is the scaling limits of CNTFET which curbs its practical applications.

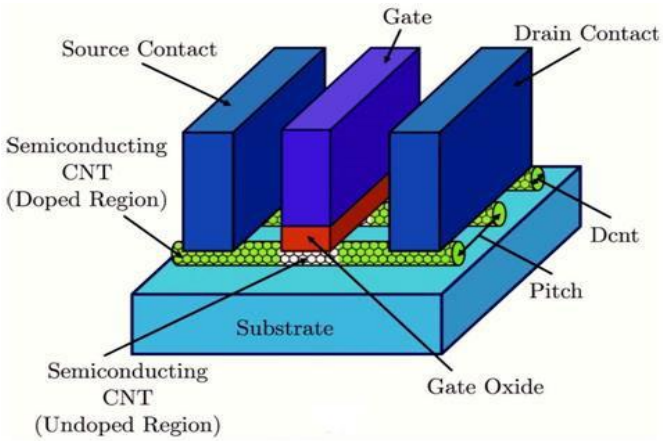

Figure 1. A typical CNTFET device [8]

Table 1. Cntfet Device Model Specification V_{dd}=1v

PARAMETER	CNTFET
Physical Channel length, L	32nm
Length of doped CNT source/drain extension region, (L_sd)	32nm
CNT Pitch	10nm
Fermi level of the doped S/D tube (E_{fo})	0.6 eV
The thickness of high-k top gate dielectric material (T_{ox})	4.0nm
Chirality of tube (m, n)	(19,0)
The mean free path in p+/n+ doped CNT = 15.0nm	15nm
The work function of Source/Drain metal contact	4.6eV
CNT work function	4.5eV
The mean free path in intrinsic CNT (Lceff)	200nm

The device model specification shown in Table 1 represents the model parameters of CNTFET. Primarily, the MOSFET logic circuits are constructed based on a generic Process Design Kit using 32nm Predictive Technology Model (PTM) with 32nm as Physical Channel Length, 1.5nm as thickness of high-k top gate dielectric material (T_{ox}) and 0.35eV as Fermi level of the doped S/D (E_{fo}). Then, the CNTFET PTM circuit models as shown in Table 1 [6] that consist of device modelling implemented in HSPICE circuit simulator [7] are being compared to the MOSFET designs.

3. PROPOSED METHODOLOGY

3.1. Proposed Low Power Adder

In the field of electronics, pass transistor logic (PTL) Rrefers to various logic families used in integrated circuit design. It curtails the tally of transistors used to compose disparate logic gates by knocking out transistors that are redundant. A full adder is proposed by modifying the existing transistor function full adder as shown in Figure 2. The adder has been restructured and reorganised by removing one PMOS transistor and NMOS transistor along with one inverter. This reduces the overall area, switching activities and power consumption in which the design becomes prominent for low-power applications.A major drawback of PTL is that when the data '0' is passed through the NMOS transistor, it is accurately received at the output and when a 5V voltage is applied to the NMOS pass transistor as data input, the output received is 5V-Vth, vice versa for PMOS.

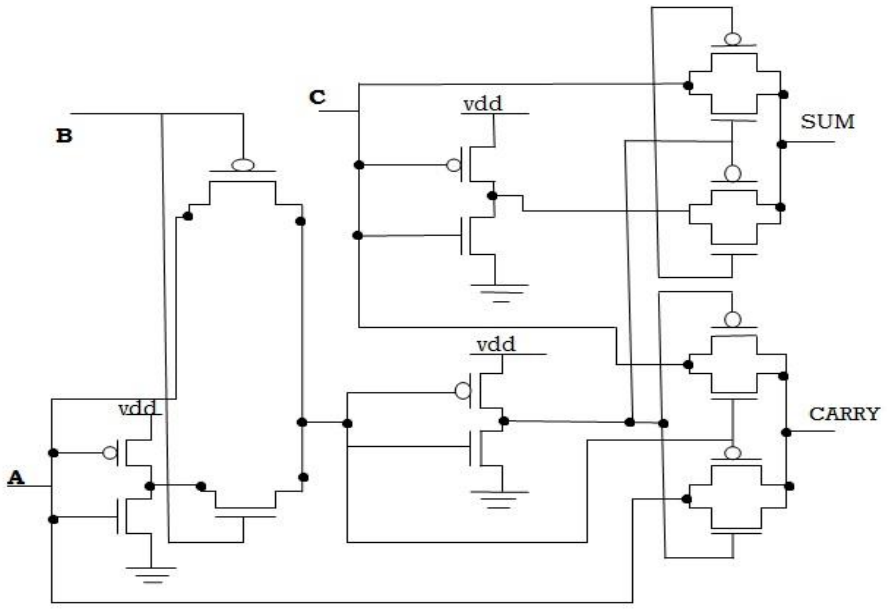

Figure 2. Proposed Low Power Full Adder

3.2. Montgomery Multiplier

Montgomery modular multiplication has found its use in major digital signal processing applications and cryptographic algorithms. The main aim of the Montgomery multiplier is to reduce the delay and enhance the security of cryptographic algorithms along with the increased speed[9][10]. The high-speed Montgomery modular multiplication algorithms and hardware architectures use the carry-save addition to prevent carry propagation at each addition operation in the add-shift loop to augment the speed, but the disadvantage is that it requires extra clock cycles which in turn make the complex hardware. The heart of the data security systems is RSA and ECC (Elliptical Curve Cryptography). However, nowadays NTRU is the most widely used algorithms in various cryptosystem play a major role in network security[11][12].Montgomery put forth an algorithm that performs the modular multiplication without conducting any trial division but still generates some residue. An exponentiation operation that intensively performs modular multiplication is referred to as modular exponentiation. The Modular multiplier gives the definite value of AxB mod M[13]. The Modular multiplier employs a 4*1 multiplexer (MUX4) and Shift Register. The shift register contains the result of first computation. The result of first computation is used to get the final output as shown in figure 3. Therefore, the Modular multiplier performs all the controls needed for the Montgomery multiplier by simply loading the register [14].

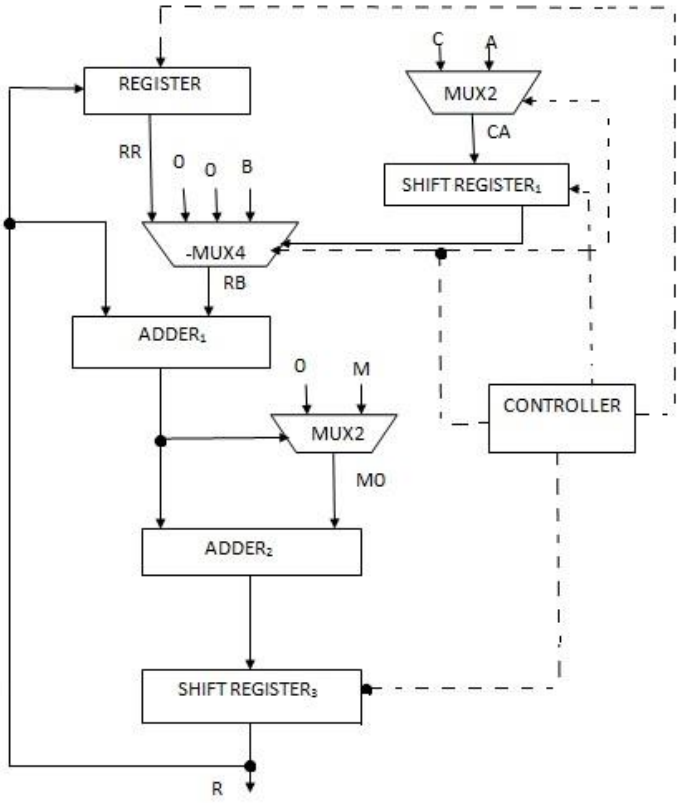

Figure 3. Montgomery Multiplier

The RSA cryptography system requires more number of modular multiplication. Montgomery multiplication is the most dynamic method is used for commutable multiplication. This method is applied to augment the encryption and decryption process [15]. The traditional way of implementing cryptosystems is application specified integrated circuit (ASIC) configuration, whereas the modern method is field programmable gate arrays (FPGA). When comparing both the methods, the latter technique proves to be highly secure and flexible[16]. Montgomery multipliers have evolved over the past few years in order to increase the speed and efficiency of several digital systems. Montgomery multiplication-based multiplier provides high throughput rate when implemented with smaller area and increased speed. This multiplier can be used in RSA cryptosystem and Elliptic Curve Cryptography as it upgrades the security as well as reduce the time consumption [17].

4. PERFORMANCE ANALYSIS

Tables 2 and 3 hold the performance analysis of both existing and proposed Montgomery multiplier 130nm and32nm CMOS and CNTFET technology. From the performance analysis the proposed low power adder and Montgomery multiplier work efficiently than the existing architecture. By the method of restructuring and recombination of circuit design, the proposed adder and multiplier maintains its benchmark with respect to high speed and low power. As shown in table the results depict the efficiency of proposed work in terms of power, speed and energy when compared to existing designs. The 32nm channel CNT can deliver output current comparable to those of the MOSFET. This is conceivable by preserving the ballistic transport over distances and the superior current density of a single CNT creating the channel. It can also be inferred that the power, delay and PDP obtained in proposed architecture of both proposed low power adder and Montgomery multiplier, the performance is much better in CNTFET technology.

Table 2. Performance Analysis of Existing and Proposed Montgomery Multiplier Using 130nm CMOS

Devices / 130nm Technology	Avg Power	Delay	Power Delay Product
		MOSFET	MOSFET
Existing PTL Adder[4]	68.59 μW	8.14ps	558.32aJ
Proposed Low power adder	63.03 μW	6.44ps	405.91aJ
Existing Montgomery Multiplier[1]	1257 μW	101.46ps	127.53fJ
Proposed Montgomery Multiplier	561.81 μW	84.41ps	47.42fJ

Table3. Performance Analysis of Existing and Proposed Montgomery Multiplier Using 32nm CMOS and CNTFET Technology

Devices / 32nm Technology	Avg Power		Delay		Power Delay Product	
	MOSFET	CNTFET	MOSFET	CNTFET	MOSFET	CNTFET
Existing PTL Adder[4]	36.15 μW	0.36 μW	9.38ps	3.51ps	339.08aJ	1.26aJ
Proposed Low power Adder	29.05 μW	0.26 μW	7.8ps	2.89ps	226.59aJ	0.75aJ
Existing Montgomery Multiplier[1]	78.04 μW	18.25 μW	113.76ps	76.02ps	8.87fJ	1.38fJ
Proposed Montgomery Multiplier	69.82 μW	12.52 μW	92.98ps	54.21ps	6.49fJ	0.67fJ

5. CONCLUSION

Montgomery multiplier is thus designed in both CMOS 130nm and 32nm as well as 32nm CNTFET technology and the performance specifications like average power, delay and the power delay product are analysed and distinguished.The operating voltage for the 130nm CMOS is 3.3V and 32nm CMOS is 1V and that of the CNTFET is 1V. All the designs are said to work at the operating frequency of 1GHz. From several analyses it has been proved that the 32nm CNTFET adder design devours fewer power when compared to 32nm CMOS circuit design. The 32nm CNTFET Montgomery multiplier circuit consumes less power when compared to 32nm CMOS design. The proposed 32nm CNTFET Montgomery Multiplier consumes 74% less power when compared to 32nm CMOS design.CNTFET is the assuring device for the future electronics as it attains the greater performance on the grounds of power, delay and power delay product. CNTFET devices are basically less prone to failure and are highly reliable.The future circuits designed with CNTFET will be a prominent one.

REFERENCES

[1] S. Meenakshi and M. Jagadeeswari, “Efficient VLSI Architecture for Montgomery Modular Multiplier”, African Journal of Basic & Applied Sciences 9 (5): 272-278, 2017

[2] MA Riyadi, I. Saad.; MT. Ahmadi, R. Ismail, “Vertical Double Gate MOSFET for Nanoscale Device with Fully Depleted Feature”, AIP Conference Proceedings, vol 1136, 248-252, 2009

[3] Rabia Qindeel, MA. Riyadi, MT. Ahmadi and VK. Arora, “Low-Dimensional Carrier Statistics in Nanostructures”, Current Nanoscience, vol. 7, pp. 235, 2011.

[4] K. S. Jitendra, A. Srinivasulu and B. P. Singh, "A new low-power full-adder cell for low voltage using CNTFETs," 9th International Conference on Electronics, Computers and Artificial Intelligence (ECAI), Targoviste, 2017, pp. 1-5.

[5] M. Zean, A. Aziz, M. Islam, M. S. M. Abir and S. Saha, "CNTFET based multiplexers and magnitude comparator," 2017 4th International Conference on Advances in Electrical Engineering (ICAEE), Dhaka, 2017, pp. 48-53.
[6] Mathan N., Vadivel M, Jayashri S," Performance metrics on ultra low power polyphase decimation filter using carbon nanotube field effect transistor technology", International Journal of Computer Aided Engineering and Technology, 10 (3), pp. 209-217, 2018.
[7] S. M. I. Huq, M. Nafreen, T. Rahman and S. Bhadra, "Comparative study of full adder circuit with 32nm MOSFET, DG-FinFET and CNTFET," 4th International Conference on Advances in Electrical Engineering (ICAEE), Dhaka, 2017, pp. 38-43.
[8] MH. Moaiyeri, RF. Mirzaee, K. Navi, O. Hashemipour, "Efficient CNTFET-based Ternary Full Adder Cells for Nanoelectronics". Nano-Micro Letters. Vol.3. No. 1. pp 43–50, 2011. DOI:10.5101/nml.v3i1.p43-50.
[9] Gang .F, "Design of modular multiplier based on improved Montgomery algorithm and systolic array", in Proc. 1st Int. Multi-Symp. Comput.Comput. Sci., vol. 2. Jun. 2006, pp. 356–359.
[10] McIvor .C, McCanny J. V and McLoone. M, "Modified Montgomery modular multiplication and RSA exponentiation techniques", IEE Proc. Comput. Digit. Techn., vol. 151, no. 6, pp. 402–408, Nov. 2004
[11] R. P. Somineni and S. M. Jaweed, "Design of Low Power Multiplier using CNTFET," 2017 IEEE 7th International Advance Computing Conference (IACC), Hyderabad, 2017, pp. 556-559.
[12] Bahram Rashidi, Sayed Masoud Sayed, Reza Rezaeianfarashahi, "High-speed hardware architecture of scalar multiplication for binary elliptic curve cryptosystems", Microelectronics Journal, vol. 52 pp. 49-65, 2016
[13] Chang K.-C, Hsu H.-W, Kuang S.-R and Wang J.-P, "Energy-efficient high- throughput Montgomery modular multipliers for RSA cryptosystems", IEEE Trans. Very Large Scale Integr. (VLSI) Syst., vol. 21, no. 11, pp. 1999–2009, Nov. 2013.
[14] Amberg. P, Harris. D. M and Pinckney. N, "Parallel high-radix Montgomery multipliers", in Proc. 42nd Asilomar Conf. Signals, Syst., Comput, Oct. 2008, pp. 772-776.
[15] Li .Z, Yang. L, Zhang S.-W and Zhang Y.-Y, "An efficient CSA architecture for Montgomery modular multiplication", Microprocessors Microsyst., vol. 31, no. 7, pp. 456–459, Nov. 2007.
[16] AH. Rezai; PK Varzi, "High-throughput modular multiplication and exponentiation algorithms using multibit-scan–multibit-shift technique", IEEE Trans. Very Large Scale Integr. (VLSI) Syst. Vol. 23 no. 9, pp. 1710–1719, 2015
[17] Sushanta Kumar Sahu and Manoranjan Pradhan, "Implementation of Modular multiplication for RSA Algorithm", IEEE Conference on Communication Systems and Network Technologies, 2011, pp. 112–114.