Proc. of the 3rd International Conference on Electrical, Communication and Computer Engineering (ICECCE)
12-13 June 2021, Kuala Lumpur, Malaysia

Performance Analysis of an Efficient Montgomery Multiplier using 7nm FinFET and Junctionless FinFET

Mathangi. R
School of Electrical Engineering
Universiti Teknologi Malaysia
Skudai, Johor, Malaysia
rmathangi@graduate.utm.my

N. E. Alias
School of Electrical Engineering
Universiti Teknologi Malaysia
Skudai, Johor, Malaysia
ezaila@fke.utm.my

Afiq Hamzah
School of Electrical Engineering
Universiti Teknologi Malaysia
Skudai, Johor, Malaysia
mafiq@utm.my

M.L.Peng Tan
School of Electrical Engineering
Universiti Teknologi Malaysia
Skudai, Johor, Malaysia
micheal@utm.my

Mathan. N
Department of Electronics and Communication Engineering
Sathyabama Institute of Science and Technology
Chennai, India
mathanmaestro@hotmail.com

***Abstract*— The digital multipliers are the assertive sources of power exhaustion in the modern digital systems. To perform most efficient arithmetic based calculations, Montgomery multiplication can be one of the best alternatives for other conventional methods in digital architecture as high-speed multipliers are desired for its remarkable performance. The main drawback of the digital multipliers is that power exhaustion is very high when compared to the other elements of the digital circuit. Shift register is the one of the most important component in a digital multiplier which consumes comparatively higher power than the other components. Shift registers contains a series of D-flip flops to store the digital data. In order to obtain a notable improvement in terms of power consumption at the chip level, the flip-flop can be modified to achieve the reduction of average power in the multiplier. The Fin-Field Effect Transistor (FinFET) is a promising candidate to overcome fundamental limitations of its Silicon based alternative MOSFET. However, there seems to be an increase in leakage power and delay. The Junctionless FinFET with uniform doping in the channel proves to offer a better performance in terms of overall speed, power consumption and power delay product. The architecture has been designed in 7nm FinFET and JL-FinFET in Synopsys HSpice and Silvaco TCAD. The results of the Montgomery Multiplier affirms that the overall energy is improved by 55% and speed of the device by 35% as compared to the existing Montgomery Multiplier.**

Keywords*— *Montgomery Multiplier, Flip Flop, Fin-Field Effect Transistor, Junctionless FinFET, Average Power, Power Delay Product.

I. INTRODUCTION

Multiplier is the basic functional unit in different VLSI circuits. Higher power consumption and low speed are the two primary restraints in the performance of the multiplier. For upgraded performance of multipliers in terms of its electrical characteristics, lot of studies has been done to fabricate devices with more advanced features [1]. Conventional MOS transistors exhibits higher power consumption and delay in the performance of the multiplier. Comprehensive studies have developed other favorable technologies like Fin-Field Effect Transistors to overcome the above said drawbacks in MOSFET [2].

The Fin-Field Effect Transistor proves to be a promising replacement for Silicon based MOSFETs as it can improve the performance of the device [3]. Though it is able to enhance the overall performance, the leakage current doesn't improve because of the presence of junctions. In order to improve the leakage current, Junctionless transistors have been introduced which tends to improve the average power and power delay product of the device [4].

In several public-key cryptosystems, the critical and time-consuming operation is the modular multiplication with large integers [5-6]. Hence, numerous arithmetic algorithms have been conferred to carry out the modular multiplication more efficiently, and Montgomery's algorithm is proved to be one of the very well know algorithm of Modular Multiplication [7]. The architecture of Montgomery Multiplier has a full adder, multiplexer, shift register and flip-flop with minimal hardware complexity [8-9].

Due to the well-balanced trade-off between area, speed and power the traditional gate flip-flop is being extensively used in modern chip design. The increase in clock loads

978-1-6654-3897-1/21/$31.00©2021 IEEE

2021 International Conference on Electrical, Communication, and Computer Engineering (ICECCE) | 978-1-6654-3897-1/21/$31.00 ©2021 IEEE | DOI: 10.1109/ICECCE52056.2021.9514146

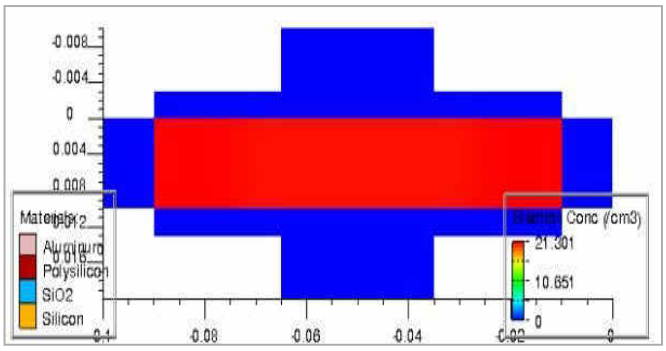

Fig 1: Device structure of 7nm JL-FinFET

because of the localized clock signal leads to higher power consumption of the digital circuit. This problem has been overcome by the single phased clocked flip flops as it reduces the dynamic power consumption with reduced clock loads. The main drawback of the single phase clocked flip flop is the

presence of repeated transistors at the internal nodes. This imposes a big challenge to achieve reduced power consumption and noticeable improvement in the overall performance. In this paper, we have proposed a novel single-phase clocked redundant transition free flip flop which has the ability to produce a satisfactory improvement in power efficiency when compared to the previously existing flip flop [10-11].

The paper is organized as: In Section II the device geometrical structure of the FinFET and Junctionless FinFET is briefly presented. Section III explains the proposed flip flop and Montgomery Multiplier, Section IV discusses about the performance analysis by comparing both FinFET and Junctionless FinFET technology, Section V provides the conclusion and future oversight of the work.

II. Device Structure and Simulation

The 3D schematic view of the n-type IM-FinFET structure is mentioned in Fig 1. The cross sectional view of Junctionless FinFET is depicted in Fig 2 which shows the uniform doping of the device across the channel. The gate length considered for the simulation is 7nm according to the ITRS technology node. HfO2 of thickness 0.6nm is used as the gate dielectric. The details of the parameters considered for the simulation is mentioned in table 1. In the Junctionless FinFET design, the uniform doping of 1 x 10^{19} is considered for source, drain and channel. Silvaco TCAD simulation tool is used to simulate both the IM mode FinFET and JL-FinFET. 3D quantum transport equations are incorporated to introduce quantum effects for channel thickness in sub 10nm regime. Band Gap Narrowing model and doping dependent model is included for highly doped JL-FinFET. Other models considered for the simulation are Band to Band tunneling model, Auger Recombination Model and Shockley-Read Hall model. For sub 10nm gate length ballistic mobility model is considered along with CVT model for carrier mobility for inversion layer.

TABLE I. DEVICE PARAMETERS

Device Parameter	Value
Gate length	7nm
Fin Width	6.5nm
Gate Oxide Thickness	0.6nm
Supply Voltage (V_{DD})	0.7V
S/D Doping	$1x10^{19}$ cm^{-3}

The circuit level analysis of the Montgomery Multiplier circuit is implemented with PTM HP 7nm FinFET by Stanford University and the process parameters is varied to make the device Junctionless. The TCAD parameters of the 7nm FinFET and Junctionless FinFET are maintained same for the SPICE model simulation for fair extraction of results. Fig 3 is the curve matching of I-V characteristics for 7nm FinFET in TCAD and SPICE and the curves seems to nearly match each other. Fin thickness is set at 6.5nm, the oxide thickness is set to 6.2nm for both cases. The outputs are shown with glitches and it can be eliminated by introducing a capacitance of 0.01nF at the output terminal.

III. Proposed Methodology

A. Proposed Low Power Flip Flop

As discussed in the introduction, the long stacked path of transistors and redundant transistor leads to increase in dynamic power consumption of the device, which in turn affects the overall performance of the shift register as well as the multiplier. In order to overcome the above mentioned challenges we have proposed a low power flip flop by modifying the existing single-phase clocked redundant transition free flip flop by restructuring and reorganizing the

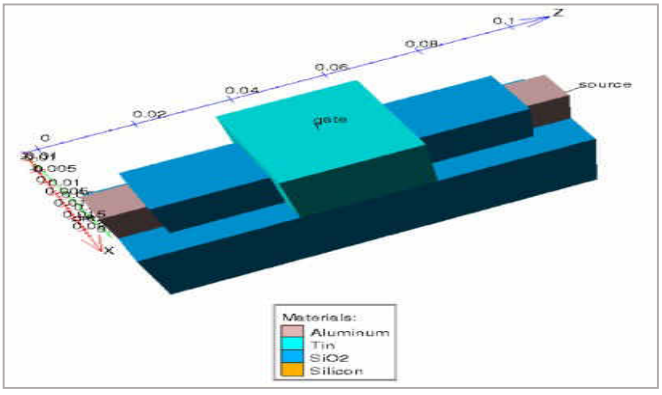

Fig 2: Device structure of 7nm JL-FinFET

existing flip flop. The proposed flip flop reduces the overall power consumption of the circuit as well as the area and switching activities which makes the device as the prominent candidate for low power applications. The schematic of the existing flip flop is mentioned in fig 4 and the proposed flop

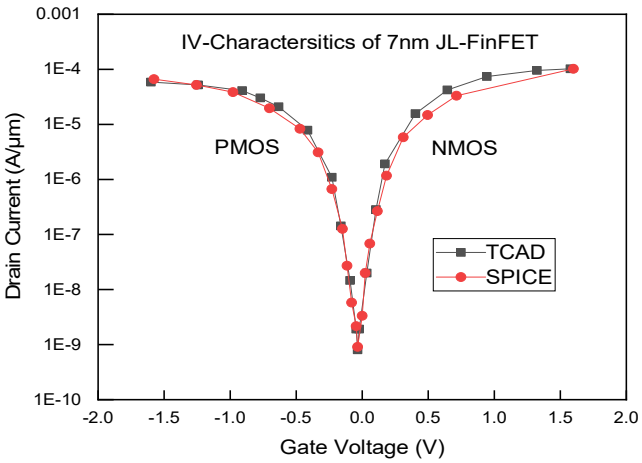

Fig 3: I-V curve of p-channel and n-channel of JL-FinFET for TCAD and SPICE model

flop in fig 5. The redundant transistors P6, N11 and N12 are removed in the proposed SRFF to reduce the area of the circuit. The discharging path of QB in the proposed SRFF is reduced when compared to the existing SRFF. The output waveform of the proposed FF is shown in fig 6.

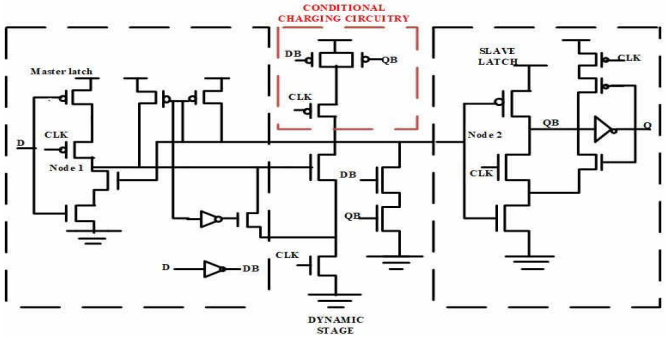

Fig 4: Schematic of the existing Single-phase clocked Flip Flop (SRFF)

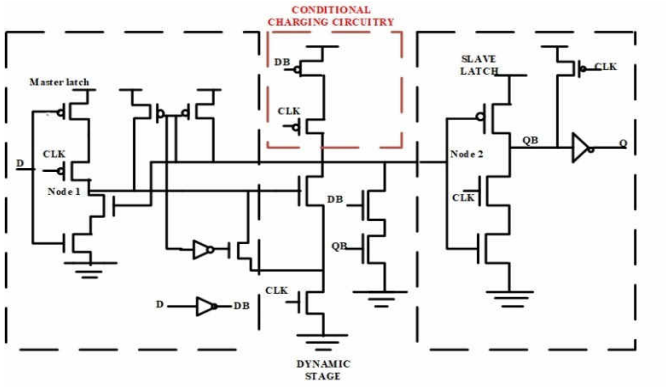

Fig 5: Schematic of the Proposed Single-phase clocked Flip Flop

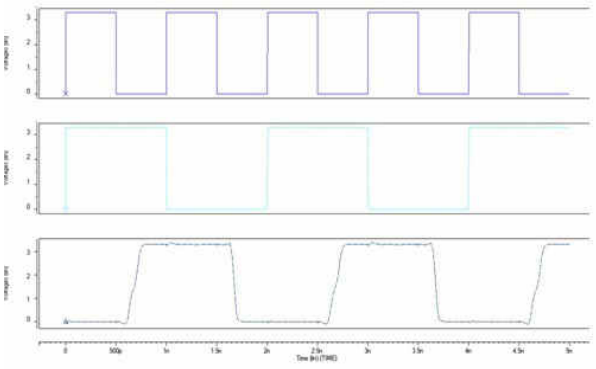

Fig 6: Waveform of the Proposed Single-phase clocked Flip Flop

B. *Montgomery Multiplier*

The digital signal processing applications and several cryptographic algorithms use Montgomery Modular Multiplication because of it reduced delay and increase in security. RSS and Elliptical Curve Cryptography are considered to be the heart of the digital data security system. Montgomery proposed a new algorithm which implements the carry save addition which reduces the carry propagation during each addition operation which increases the speed of the multiplier without conducting the trial divisions. The architecture of Montgomery multiplier is illustrated in fig 7 which consists of 14T Full Adder along with the proposed SRFF, 4x1 mux and Serial in Serial out Shift Register. The task of Shift Register is to store the result of the first computation and release it when the clock signal is given to get the final output. By using this technique high throughput rate with efficient performance is achieved.

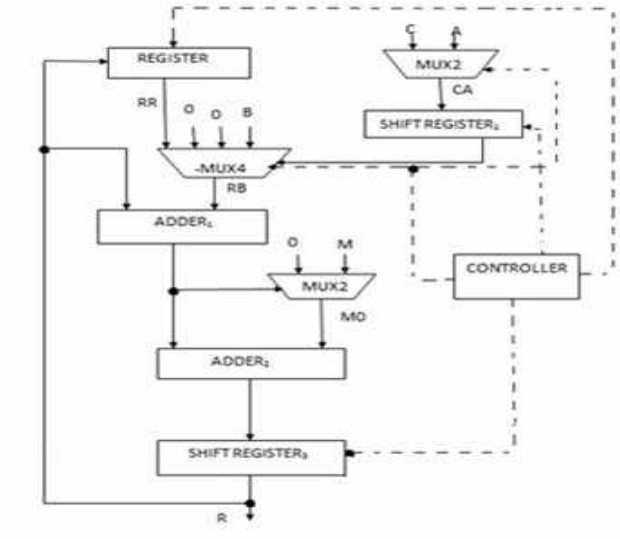

Fig 7: Schematic circuit of Montgomery Multiplier [9]

TABLE 2: PERFORMANCE ANALYSIS OF FinFET AND JL-FinFET BASED MONTGOMERY MULTIPLIER

Devices 7nm Technology	Avg Power (µW)		Delay(ps)		Power Delay Product	
	FinFET	**JL-FinFET**	**FinFET**	**JL-FinFET**	**FinFET**	**JL-FinFET**
Existing LFF	4.084	2.58	10.25	8.55	41.86aJ	22.05aJ
Proposed LFF	3.001	1.45	9.85	7.25	29.55aJ	10.51aJ
Existing Montgomery Multiplier	96.89	79.12	125.68	101.44	12.77fJ	8.02fJ
Proposed Montgomery Multiplier	75.24	59.25	75.59	68.45	5.6fJ	4.05fJ

IV. PERFORMANCE ANALYSIS

The performance analysis of the existing and proposed Montgomery multiplier for 32nm and 7nm technology FinFET technology is mentioned in Table 2. From the performance analysis we can notice that the proposed low power flip flop when implemented in the Montgomery Multiplier works efficiently than the existing architecture. Table 2 indicates the performance analysis of FinFET-based and JL-FinFET-based Montgomery Multiplier.

The average power consumption from the source is obtained for each circuit in the multiplier. Junctionless FinFET shows a significant reduction of 20.3% in average power than its counter-part IM-FinFET because of its excellent transport properties. The IM- FinFET has the increased leakage current because of the presence of junctions.

The inversion mode FinFET shows highest propagation delay than the other FET because of its developed design metrics that leads to less leakage current for sub 10nm channel length. The Power Delay Product is the product of average power and delay in the circuit. In 7nm technology, IM-FinFET consumes the higher power 15.3% when compared to the Junctionless FinFET and hence it has the maximum PDP. As the first two parameters, average power and delay are lesser for JL-FinFET it has comparatively smaller PDP. The output waveforms of Montgomery multiplier and 4x1 mux is given in Fig 8 & Fig 9.

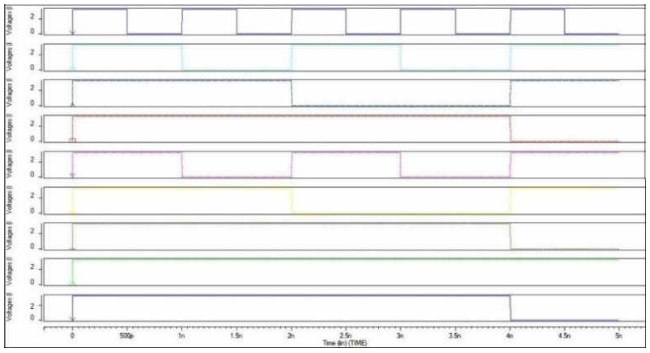

Fig 8: Output of 7nm JLFinFET based Montgomery Multiplier

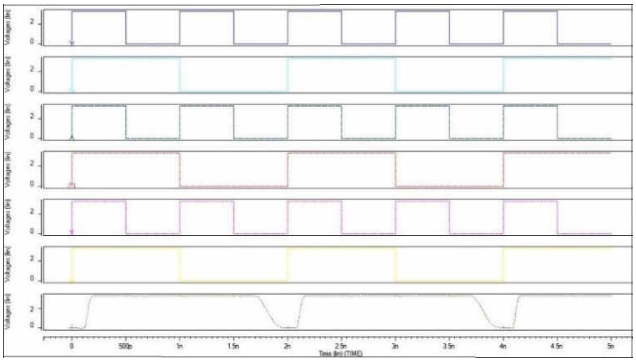

Fig 9: Output of 7nm JLFinFET based 4x1 Multiplexer

V. CONCLUSION

In conclusion, this paper observed the performance of Montgomery Multiplier in 7nm IM-FinFET and Junctionless FinFET are investigated. The proposed flip flop performs around 55% better than the existing flip flop. It is found that in terms of average power, power delay product and delay, the proposed multiplier performs well when implemented in 7nm Junctionless FinFET when compared to the Inversion mode FinFET.

ACKNOWLEDGMENT

The authors gratefully acknowledge the Ministry of Higher Education (MOHE), Malaysia for the financial support under the Fundamental Research Grant Scheme: FRGS/1/2019/STG07/UTM/02/3. Besides, thanks to the Research Management Center (RMC) of University Teknologi Malaysia (UTM) for accommodating an excellent research environment to accomplish this work.

REFERENCES

[1] Meenakshi, S., & Jagadeeswari, M. (2017). Efficient VLSI Architecture for Montgomery Modular Multiplier. *African Journal of Basic & Applied Sciences*, *9*(5), 272-278.J. Clerk Maxwell, A Treatise on

Electricity and Magnetism, 3rd ed., vol. 2. Oxford: Clarendon, 1892, pp.68–73.

[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] Qindeel, R., A Riyadi, M., Taghi Ahmadi, M., & K Arora, V. (2011). Low-dimensional carrier statistics in nanostructures. *Current Nanoscience*, *7*(2), 235-239..

[4] Shylashree, N., Venkatesh, B., Saurab, T. M., Srinivasan, T., & Nath, V. (2019). Design and analysis of high-speed 8-bit ALU using 18 nm FinFET technology. *Microsystem Technologies*, *25*(6), 2349-2359.M.

[5] Karunatilaka, D., Zafar, F., Kalavally, V., & Parthiban, R. (2015). LED based indoor visible light communications: State of the art. *IEEE Communications Surveys & Tutorials*, *17*(3), 1649-1678.

[6] Colinge, J. P., Lee, C. W., Akhavan, N. D., Yan, R., Ferain, I., Razavi, P., ... & Yu, R. (2011). Junctionless transistors: physics and properties. In *Semiconductor-On-Insulator Materials for Nanoelectronics Applications* (pp. 187-200). Springer, Berlin, Heidelberg.

[7] Lamba, B., & Sharma, A. (2018, January). A review paper on different multipliers based on their different performance parameters. In *2018 2nd International Conference on Inventive Systems and Control (ICISC)* (pp. 324-327). IEEE.

[8] Bonpapa, J. C., & Reddy, U. P. (2015). Design and Performance Analysis of multipliers using different logic styles. *International Journal of Engineering Research & Technology (IJERT)*, *4*(04).

[9] Mathan, N., Jayashri, S., Alias, N. E., & Tan, M. L. P. (2019). Performance Analysis of Montgomery Multiplier using 32nm CNTFET Technology. *Indonesian Journal of Electrical Engineering and Informatics (IJEEI)*, *7*(4), 697-702.

[10] Clark, L. T., Vashishtha, V., Shifren, L., Gujja, A., Sinha, S., Cline, B., ... & Yeric, G. (2016). ASAP7: A 7-nm finFET predictive process design kit. *Microelectronics Journal*, *53*, 105-115.

[11] Chen, L., Sun, Y., & He, W. (2017, October). Low-power single-phase clocked redundant-transition-free flip-flop design with conditional charging scheme. In *2017 IEEE 12th International Conference on ASIC (ASICON)* (pp. 916-919). IEEE.