Scientific Journal Impact Factor (SJIF) : 1.711
International Journal of Modern Trends in Engineering and Research
ISSN (ONLINE) : 2349 - 9745
ISSN (PRINT) : 2393 - 8161

Implementation of Processing Element for Modular Multiplier Using Static CMOS and Multiplexer Logic Circuit at 65nm

Yamini Banjare[1], Vishal Moyal[2]

[1,2]*Department of Electronics and Telecommunication Faculty of Engineering & Technology, Shri Shankaracharya Technical Campus, Bhilai ,C.G*

Abstract- Many public key cryptographic algorithms require modular multiplication of very large operands as their core arithmetic operation. In this paper fast processing and low power consuming processing element of modular multiplier hardware is proposed. Proposed processing element is implemented of 4 bit in 65nm technology using static CMOS and multiplexer logic. The processing element designed using static CMOS logic consumes 1.2246uw power and multiplexer logic consumes 0.939uw with 1.2volt operating voltage and 1 fF capacitor. The number of transistor in static CMOS logic contains 58T and multiplexer logic contains is 42T. The multiplexer logic based processing element consumes 23% less power than the static CMOS.

Keywords- Processing element**,** Modular multiplier, Montgomery's algorithm, Static CMOS, Multiplexer.

I. INTRODUCTION

Finite field multiplication is a fundamental operation for many cryptographic algorithms including RSA, digital signature algorithm and elliptic curve (ECC). Modular multiplication[9] can be performed with in an ordinary multiplication followed by remainder computation, where the product is divided by the modulus. Now a day's Montgomery multiplier[10] are more successful. Modular multipliers are most the important arithmetic function in public key cryptosystem because they are most used once and require large moduli, therefore computational method to accelerate, reduced energy consumption and simplify the use of such operation especially in hardware are always of great value for system that require data security. A scalable Montgomery multiplier uses a small processing element with fixed word size. This processing element is the main functioning element so it should consumes low power and response faster. Great attention has been focused on low power microelectronics due to the rapid development of laptops, smart phone, portable systems and cellular networks. Low power consumption is the major consideration in circuit design. adder are the core elements of complex arithmetic circuits as they widely used in arithmetic logic units and multipliers.

In this paper processing element of modular multiplier is designed and implemented using static CMOS and multiplexer to reduce the power of processing element of modular multiplier. complementary metal oxide semiconductor (CMOS) is primary technology. Power consumption of CMOS [7] consists of dynamic and static components. Dynamic power is consumed when transistor is switching and static power dissipation is due to leakage mechanism. Dynamic power dissipation is reduced by using less transistor ,as less transistor are used it will take less area as well as less switching operation can be performed.

The processing element is designed using multiplexer[1][2][3][4]as on multiplication design adder is most important circuit. In adder circuit XOR gate is important circuit ,so XOR circuit with less number of transistor, power consumption and delay are highly desirable on VLSI system.

II. PREVIOUS WORK ON PROCESSING ELEMENT

An encryption accelerator reconfigurable Montgomery multiplier [9] circuit design was proposed by Mathew et al. they designed a scalable Montgomery multiplier by using small processing element with a fixed word size multiple times to process very long operands.

Processing element

This used a carry save adder (CSA) to add the partial product word to the accumulating result Z and second CSA was used to conditionally add in the modulus M, after testing the 'odd' bit. The odd bit is computed and stored in the first cycle of each outer–loop iteration system throughput was increased by processing the accumulating result Z in carry save redundant form within the loops, and converting to non redundant binary form in the last cycle of the inner loop (j=e), prior to storage in the register. They had designed Processing element using static CMOS. This processing element having three main parts as follows:

1. Sum generation : this sum generation block contains 4 input XOR gate. First sum generation circuit added all the four bit and given sum of the 4 input. Second sum generation circuit are used for adding the previous sum, carry and modulus value. This whole circuit was designed using static CMOS logic.
2. Carry generation: this carry generation block contains carry generation circuit, designed through static CMOS logic. First carry generation circuit generated carry of the four inputs. second carry generation circuit was used for performing same procedure with modulus value.
3. Modulus: this design had modulus value and this modulus value is added with previous sum and carry, when the product is odd.

III. IMPLEMENTATION OF PROCESSING ELEMENT

This paper main focus is reducing power of the processing element hence two different designs are implemented in 65nm technology. First design method, using static CMOS and second design method, using multiplexer. Block diagram of proposed circuit is shown below

3.1. Processing element using static CMOS design

After studying the previous work on processing element we focus on improving the design of sum generation and carry generation circuit.previously this processing element was implemented in 90nm technology, so this design is implemented in 65nm technology using static CMOS.the schematic diagram of the implemented circuit is given in figure 1(a). the functioning of the processing element is firstly apply input bits in the adder circuit and sum and carry are parallely generated, so that computation time has been reduced and complexity of the circuit has been also reduced. This proposed processing element has two main blocks sum generation and carry generation.

Sum generation: this sum generation block contains 4 input XOR gate. First sum generation circuit adds all the four input bit and given sum. Second sum generation circuits are used for adding the previous sum, carry and modulus value. This whole circuit was designed using static CMOS logic.

Carry generation: this carry generation block contains carry generation circuit, designed through static CMOS logic. First carry generation circuit generated carry of the four inputs. Second carry generation circuit was used for performing same procedure with modulus value.

3.2. Processing Element using Multiplexer Logic Design

In complementary metal oxide semiconductor (CMOS) technology, reducing the length of channel to below about 65nm leads to critical problems and challenges such as decreasing gate control, short

channel effect, high power density, high sensitivity to process variation and exponential leakage current increment. For this reasons reducing the transistors size finally will stop at a point, leading to taking advantage of new technologies that do not have above problems may be felt. The vast use of this operation in arithmetic functions attracts many researchers to this field. Multiplexer circuit reduces the number of transistor as well as the complexity of the circuit. As the transistor count are reduced the switching transition so power dissipation of the circuit is also reduced. The schematic design of the processing element is shown in figure 2 (a).

Processing element using multiplexer contains following blocks:

Adder: adder circuit is designed for using four input XOR gate. This XOR gate has designed using multiplexer logic. In this four bit XOR gate 3 multiplexer are used. In this adder circuit carry generation circuit is inbuilt and this carry generation circuit is also implemented using multiplexer logic. Three multiplexer are used for implementing carry generator. this design use the 4-T XOR gate and 6-T carry generator.

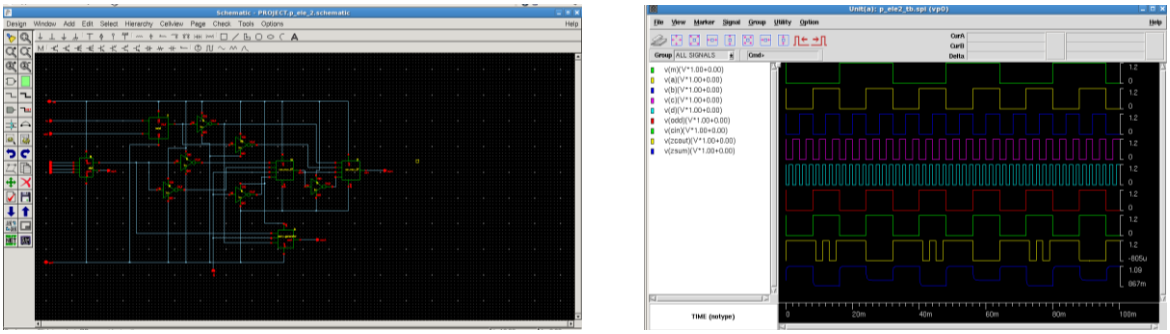
Sum generation: this sum generation module use the three input XOR gate for adding modulus value in the previous sum. Modulus value is added in the circuit if the product output is odd.

Carry generation: this carry generation module generated the carry when the modulus bit is added on the sum generation module. This circuit is also implemented using multiplexer logic hence the power consumption is reduced.

IV. RESULT AND DISCUSSION

The processing element is designed and simulated using Zeni-EDA tool at SMIC 65nm technology. The schematic and simulation result of the all two design methods are shown below-

1. Schematic of the processing element using static CMOS circuit is shown in below figure:

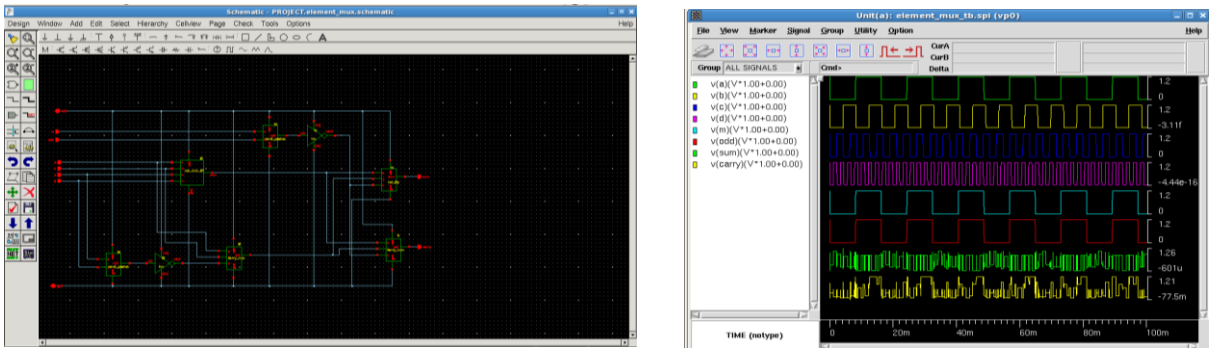


(a) (b)

Figure 1. Schematic and simulation result of processing element using static CMOS.(a) schematic (b) simulation

This schematic circuit (a) contains one four input adder circuit, one NAND gate, five inverter, one sum generation circuit and one carry generation circuit. This circuit consumes 1.2246uw dynamic power. In simulation waveform is plotted between voltages and time period.tis simulation shows the modulus (m), input signals (a),(b),(c),(d),carry signal (cin) and output signals (sum) and (carry).

2. Schematic of processing element using multiplexer is shown in below figure:



(a) (b)

Figure 2. schematic and simulation of processing element using multiplexer. (a) schematic (b) simulation.

This schematic circuit (a) contains one four input adder circuit, one NAND gate, five inverter, one sum generation circuit and one carry generation circuit. This circuit consumes 0.939 uw dynamic power. In simulation waveform (b) is plotted between voltages and time period.tis simulation shows the modulus (m), input signals (a),(b),(c),(d),carry signal (cin) and output signals (sum) and (carry).

V. CONCLUSION

This paper shows the implementation of the processing element of the modular multiplier using static CMOS and multiplexer. This paper shows that processing element designed using multiplexer reduce the number of transistor as well as reduces power dissipation upto 20%.

REFERENCES

[1] Ji -ZhongSHEN Yi WEI, "Design of a novel low power 8-transistor 1-bit full adder cell," in *journal of Zhejiang university*, 2011, pp. 604-607.

[2] H.T, Waang,Y. Bui, "design and analysis of low power 10 transistor full adders using novel XOR-XONR gates," in *IEEE tran.circ.syst*, pp. 25-30.

[3] Sandeep K. Arya, Sujata Pandey Manoj Kumar, "Single bit full adder design using 8 transistors with novel 3 transistor XNOR," in *International Journal of VLSI design & Communication Systems (VLSICS) Vol.2, No.4*, December 2011.

[4] Rajesh Mehra2 Pooja Singh, "Design Analysis of XOR Gates Using CMOS & Pass Transistor Logic," in *International Journal of Engineering Science Invention Research & Development*, 2014.

[5] Bijoy Kundu, Sovan Ghosh, Vinay Kumar Partha Bhattacharyya, "Performance Analysis of a Low-Power High-Speed HYBRIDE 1-BIT FULL ADDER CIRCUIT," in *IEEE TRANSACTIONS ON VERY LARGE SCALE INTEGRATION (VLSI) SYSTEMS, VOL. 23, NO. 10*, 2015.

[6] Kumar, and M. A. Bayoumi S. Goel, "“Design of robust, energyefficient Full adders for deep submicrometer design hybrid cmos lgic style," in *IEEE Trans. Very Large Scale Integr. (VLSI) Syst., vol. 14*, 2006, pp. 1309–1321

[7] D. Harris, and A. Banerjee, N. H. E. Weste, "CMOS VLSI Design:A Circuits and Systems Perspective, 3rd ed," in *pearson education* , 2006.

[8] T. K. Darwish, and M. A. Bayoumi, A. M. Shams, "“Performance analysis of low-power 1-bit CMOS full adder cells,”," in *IEEE Trans. Very LargeScale Integr. (VLSI) Syst., vol. 10, no. 1*, 2002, pp. 20–29.

[9] David Harris, Mark Anders,Steven hsu,Ram krishnamurthy Sanu Mathew, "A 2.4GHz 256/1024 bit Encryption Accelelator Reconfigurable Montgomery Multiplier in 90 nm CMOS," in *IEEE int. soc.conf, hsinshu*, taiwan, 2007, p. 25_28.

[10] o.nibouche. A. bourindue and M. Nibouche, "Architecture for Montgomery's Muiltiplier," in *IEEE proc. Computer digital tech*, 2003, pp. 361-368.