© 2017 IJSRSET | Volume 3 | Issue 1 | Print ISSN: 2395-1990 | Online ISSN : 2394-4099
Themed Section: Engineering and Technology

Low-Power and Area Efficient Dual Dynamic Node Pulsed Hybrid Flip-Flop

P. Arun Kumar, C. Yamunarani

Department of Electrical and Communication Engineering, SNS College of Technology, Tamilnadu, India

ABSTRACT

Elliptic curve point multiplication (ECPM) is one of the most critical operations in elliptic curve cryptography. In this brief, a new hardware architecture for ECPM over GF(p) is presented, based on the residue number system (RNS). The proposed architecture encompasses RNS bases with various word-lengths in order to efficiently implement RNS Montgomery multiplication. Two architectures with four and six pipeline stages are presented, targeted on area-efficient and fast RNS Montgomery multiplication designs, respectively. The fast version of the proposed ECPM architecture achieves higher speeds and the area- efficient version achieves better area–delay tradeoffs compared to state- of-the-art implementations.

Keywords : Elliptic curve cryptography (ECC), Montgomery multiplication, residue arithmetic, residue number system (RNS).

I. INTRODUCTION

Due to the modern deep-pipelined architectures in VLSI, power dissipation has been considered as one of the major concerns. Thus, besides primary concerns of the VLSI circuit design such as area, performance and cost, the static power dissipation has also become an active area of research. This is mainly due to the enhancement of chip scale of integration and the steady improvement of the operating frequency. The excessive static power dissipation in integrated circuits discourages their use in a portable device and also causes overheating which degrades the system performance and lifetime. Static Power dissipation has a direct impact on the packaging cost of the chip and coding cost of the system. All of these factors drive the VLSI system designers to consider the static power dissipation as a major issue and to reduce the circuit static power dissipation.

At present scenario Field-programmable gate arrays (FPGAs) architectures are the popular preference for digital circuit implementation. In this architecture the programmable routing switch topology is used to connect three other wires in adjacent channel segments of FPGA routing architecture. This overhead in the present architecture is the static power dissipation associated with the routing switch. Extensive work has been dedicated to get better the performance of the routing switch (Kunwar Singh et al., 2014). The clocking system is one of the major power consuming components in VLSI system. The present research mainly focuses on efficient routing switch design for achieving lower power static dissipation

II. METHODS AND MATERIAL

1. Problem Formulation

Static Power dissipation has become an important issue in modern VLSI design. This is mainly due the enhancement of chip scale of integration and the steady improvement of the operating frequency. The excessive static power dissipation in integrated circuits discourages their use in a portable device and also causes overheating which degrades the system performance and lifetime. Static Power dissipation has a direct impact on the packaging cost of the chip and coding cost of the system as discussed in Roy & Prasad (2009). All of these factors drive the VLSI system designers to consider the power dissipation as a major issue and to reduce the circuit static power dissipation.

A huge portion of the power is consumed by FPGA routing switch consists of multiplexer, a buffer and SRAM configuration cells.FPGA routing switch circuit is completely based on how the interconnection is done and those interconnection delays dominates the logic delays. In classical models, all the wires run along orthogonal grid lines with uniform separation .The routing problem minimization is made use of switch box to find out the existing possible solution .Three different modes of operation in FPGA design helps to overcome the drawback of the existing method which in turn helps to lower the FPGA routing static power dissipation. Finite wire length is an important aspect in routing which helps to reduce the path delay in lower power routing switches. Static Power dissipation is reduced in low-power mode due to optimization in Power-delay product (PDP) which switches the routing switches and operated on different modes.

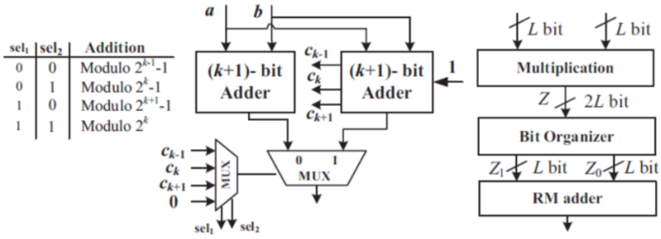


Figure 1. Proposed RM adder

In this paper, a hierarchical interconnect architecture is introduced by making use of low-swing long wires which helps to reduce power dissipation. In turn, predefined dual Vdd and dual Vt has provided the possibilities to reduce static power which plays a major role in power optimization as shown in Figure 2.1. The increase in the supply voltage leads to higher performance of the circuit, but in turn increases static power dissipation. Through Vdd scaling, we will be able to lower the supply voltage which is passed to the entire design to reduce static power dissipation. Alternatively, dual-Vdd provides high supply voltage (VddH) on critical paths and low supply voltages (VddL) for non critical paths .The proposed new switch design is based on the observations, how those switches which drives input signals to the logical blocks. The switch includes n-MOS and p-MOS sleep transistors in parallel. Power in the gating structure which is operated in different operating modes is designed through the parallel clamped PMOS with NMOS tree structure .Voltage gap of MOS transistors are reduced when they are connected in parallel. In turn in increases the leakage power dissipation is more in the system. In this section, we propose a circuit which consist of P-MOS and N-MOS switches. We propose a circuit under Mode-I, Mode-II and Mode-II based write driver circuit on 6T and 10T SRAM which optimizes power using a single routing switch. It operates on three modes Active, sleep and drowsy.

A. Objectives

The objectives of this thesis are:

1. To develop novel routing switch designs through Mode-I, Mode-II , Mode-II routing switch using 6T SRAM and Mode-II routing switch with write driver circuit using 10T SRAM to optimize the static power dissipation
2. To evaluate the performance of the proposed routing switch design with write driver circuits with other existing designs in the literature.
3. To evaluate the significance and potential of the proposed routing switch design with write driver circuit with the performance metrics like static power dissipation, PDP, Energy delay product (EDP), and static current are provided.

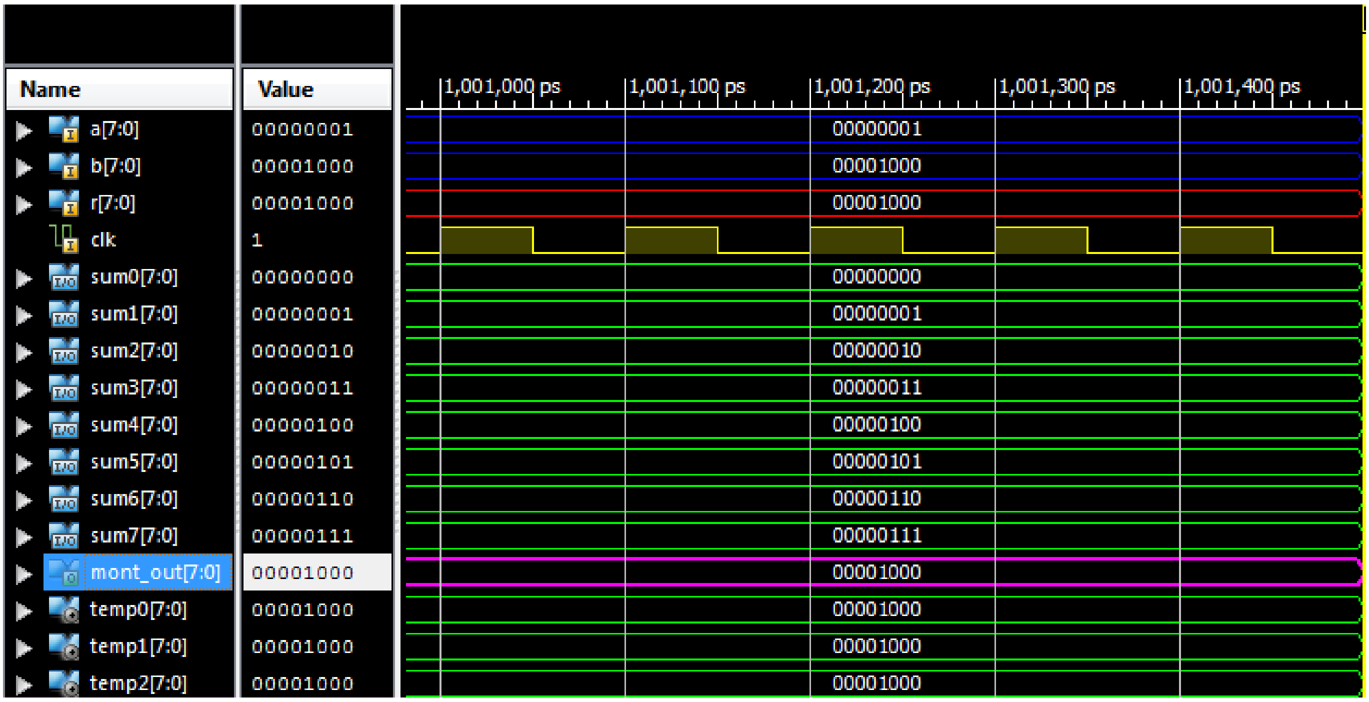
B. Research Contribution and Methodology

The present research work has develops Four novel routing switch designs for minimizing the static power dissipation in the FPGA routing switch design. The four proposed routing switch designs are explained clearly in the following sections.

- Low Power FPGA Routing Switch.
- FPGA Routing Switch For Mode-I Operation.
- FPGA Routing Switch For Mode-Ii Operation.
- FPGA Routing Switch With Write Driver On 6t And 10t Design.

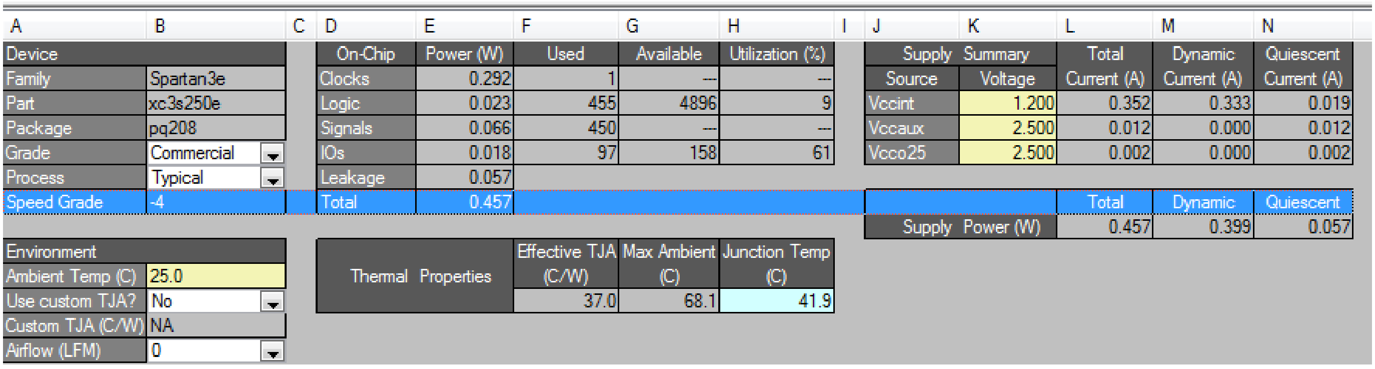
III. RESULTS AND DISCUSSION

The proposed routing switch is analyzed based on the previously designed traditional routing switch methodology in which the rise and fall times of the buffer are equal. The output response with respect to input parameters of the multiplexer is analyzed and the power characteristics of the proposed switch are simulated using Spice tool. The current drawn from various sources such as the multiplexer, SRAM configuration cells and sleep transistors consumes power and the corresponding values are tabulated as shown in Table I. The tabulated results show the proposed routing switch offers large leakage current reduction which is operated at high speed than the traditional switch design. In mode-II static power is much high when compare to existing FPGA routing due to higher switching activity between active and sleep mode. This in turn increases static power in single circuitry node.



Name	Value
a[7:0]	00000001
b[7:0]	00001000
r[7:0]	00001000
clk	1
sum0[7:0]	00000000
sum1[7:0]	00000001
sum2[7:0]	00000010
sum3[7:0]	00000011
sum4[7:0]	00000100
sum5[7:0]	00000101
sum6[7:0]	00000110
sum7[7:0]	00000111
mont_out[7:0]	00001000
temp0[7:0]	00001000
temp1[7:0]	00001000
temp2[7:0]	00001000

Figure 2. Shows the output waveform



A	B
Device	
Family	Spartan3e
Part	xc3s250e
Package	pq208
Grade	Commercial
Process	Typical
Speed Grade	-4

On-Chip	Power (W)	Used	Available	Utilization (%)
Clocks	0.292	1	---	---
Logic	0.023	455	4896	9
Signals	0.066	450	---	---
IOs	0.018	97	158	61
Leakage	0.057			
Total	0.457			

Supply Source	Summary Voltage	Total Current (A)	Dynamic Current (A)	Quiescent Current (A)
Vccint	1.200	0.352	0.333	0.019
Vccaux	2.500	0.012	0.000	0.012
Vcco25	2.500	0.002	0.000	0.002
		Total	Dynamic	Quiescent
Supply Power (W)		0.457	0.399	0.057

Environment	
Ambient Temp (C)	25.0
Use custom TJA?	No
Custom TJA (C/W)	NA
Airflow (LFM)	0

Thermal Properties	Effective TJA (C/W)	Max Ambient (C)	Junction Temp (C)
	37.0	68.1	41.9

Figure 3. Show the performance characteristics, speed and its ambient temperature

The proposed mode-I technique outperforms in all distinct three modes of operation such as sleep, active and drowsy than the existing FPGA routing mode of operation. When sleep enabled, tri state circuit operates depending on level of input pulses. If drowsy negative feedback pulses generates which block the circuit from grounding, when sleep or drowsy circuit is in active mode. But under a condition when Sleep = 0 and drowsy is high, then circuit becomes drowsy at this condition power leakage is high and to overcome the power losses in the circuit, transistors are reduced to decline losses. The proposed Mode-II technique optimizes static power dissipation when compare to mode-I by removing the unwanted switching activity caused by drowsy mode. Besides it reduces the number of transistors when compare to mode-I based routing switch. Average power dissipation is reduced in mode-I when compare to existing FPGA routing switch by reducing the unwanted switching activities that occur due to dual Vdd power supply(sleep and sleepb)(Anderson J, Najm F, 2009).In proposed mode-II routing network is smaller when compare to mode-I which reduces the average power dissipation.

Further in order to optimize the static power further the traditional 6T and 10T SRAM cell structures are implemented in standard 180 nm CMOS technology. Both the cells have have the identical sense amplifier design, address decoders and data line drivers. But in case of 10-T SRAM cell the write mode is controlled by write circuitry which helps to reduce the switching activity of the transistor. Read/Write operations have been simulated and the performance of the newly proposed cell is evaluated as shown in Table II. The proposed design write power is reduced up to 6% by lowering the switching activity of transistors has a significantly less write power dissipation than the conventional method. The 6T SRAM based mode-II design power dissipation is much higher when compared to that of the new design. The proposed design write power is reduced up to 6% by lowering the switching activity of the transistor when compared to existing 6-T SRAM cell design [12]. However, when the core SRAM cell is activated the circuit components present in the structure consumes short pulse current and after few ps, it becomes 0. As the write circuitry helps to reduce the unwanted the switching activity of the transistors in 10T SRAM based mode-II design with write driver makes the proposed method has measurable power reduction in the SRAM cell structure. This ensures that the power dissipation is no longer a bottleneck design during write operation [13]. During the standby mode of the transistor, static leakage current is the primary parameter for the nanoscale SRAM cell of the routing switch architecture of FPGA [13]. Although the proposed 10T based Mode-II design with write driver has more transistor count, our word line evaluation voltage of 0V incurs no added leakage current of the SRAM cell. Besides, the pull-down transistors are less significant than those in the conventional SRAM cell, hence its leakage is reduced. [14-15]. By comparing the leakage current of the two designs, the proposed cell leakage is about 9% less than that of the conventional 6-T SRAM cell structure. In PDP, if D represents delay and P represents power consumption of the circuit then the metric can be expressed as PDP (energy) = Power (P)×Delay (D). The EDP (Energy Delay Product) can be estimated by multiplying Energy with average D-to-Q. If power is the higher priority than both EDP and PDP matrices may not provide better solutions.

IV. CONCLUSION

This research work proposed four novel Routing switch designs for minimizing the static power dissipation in the FPGA routing circuits. In this paper, four new routing switch designs are analyzed which are designed to operate in high power, low power and sleep mode. The proposed switch offers less static power dissipation compared to the existing architecture. By eliminating the unwanted switching activity, the revised structure of the proposed Mode-II based switch design, which outperforms the CLK driving power and internal power dissipation. The proposed mode-II design which efficiently removes the unwanted switching activity caused by drowsy state which has shown in mode-I, this results less static power dissipation. The static current, EDP and PDP variation performances of the designs were studied in detail. The results show that average static power reduction of 4.5% is achieved in mode-I and in 5% is achieved in mode-II than existing FPGA routing switch. Power results are analyzed 0.18um and tested with supply voltage of 1.8V.Further in order to reduce static power further a novel 10T SRAM based mode-II with write driver circuitry is proposed and analyzed. The read and write operations of the SRAM cell structure have power dissipation setback during the write cycle, which is controlled by writing driver circuitry. As an outcome, power dissipation is reduced 6% than that of the existing 6T SRAM based mode-II design. At the same time, the proposed design minimizes 6% cell leakage and 9% static power dissipation than the Mode-II based 6T SRAM design approach. The performance improvements specify that the proposed Designs are appropriate for modern high-performance routing switch FPGA design where power dissipation is of major Concern.

V. REFERENCES

[1]. N. Koblitz, "Elliptic curve cryptosystems," Math. Comp., vol. 48, no. 177, pp. 203–209, 1987.

[2]. V. S. Miller, "Use of elliptic curves in cryptography," in Proc. Adv. Cryptology LNCS, 1986, pp. 47–426.

[3]. I. Blake, G. Seroussi, and N. Smart, Elliptic Curves in Cryptography. Cambridge, U.K.: Cambridge Univ. Press, 2002.

[4]. D. M. Schinianakis, A. P. Fournaris, H. E. Michail, A. P. Kakarountas, and T. Stouraitis, "An RNS implementation of an F p elliptic curve point multiplier," IEEE Trans. Circuits Syst. I, Reg. Papers, vol. 56, no. 6, pp 1202–1213, Jun. 2009.

[5]. C. J. McIvor, M. McLoone, and J. V. McCanny, "Hardware elliptic curve cryptographic processor over GF(P) ," IEEE Trans. Circuits Syst. I, Reg. Papers, vol. 53, no. 9, pp. 1946–1957, Sep. 2006.

[6]. G. Orlando and C. Paar, "A scalable GF(P) elliptic curve processor archi- tecture for programmable hardware," in Proc. Workshop Cryptograph. Hardware Embed. Syst. LNCS, 2001, pp. 348–363.

[7]. S. B. Ors, L. Batina, B. Preneel, and J. Vandewalle, "Hardware imple- mentation of an elliptic curve processor over GF(P) ," in Proc. IEEE Appl.-Specific Syst. Arch. Process., Jun. 2003, pp. 433–443.

[8]. N. Guillermin, "A high speed coprocessor for elliptic curve scalar multiplications over Fp ," in Proc. CHES 12th Int. Conf. Cryptograph. Hardware Embed. Syst., 2010, pp. 48–64.

[9]. S. Kawamura, M. Koike, F. Sano, and A. Shimbo, Cox Rower Architec- ture for Fast Parallel Montgomery Multiplication. New York: Springer-Verlag, 2000, pp. 523–538.

[10]. J. C. Bajard, M. Kaihara, and T. Plantard, "Selected RNS bases for modular multiplication," in Proc. IEEE 19th Int. Symp. Comput. Arith., Jun. 2009, pp. 25–32.