Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 70 (2015) 355 – 361

Procedia
Computer Science

4th International Conference on Eco-friendly Computing and Communication Systems, ICECCS 2015

# Low Power Modulo$2^n$ +1 Multiplier Using Data Aware Adder Tree

R.Sakthivel[a], M.Vanitha[b], Kishore Sanapala[a], K.Thirumalesh[a]

[a]School of Electronics Engineering,VIT University,Vellore-632014,India
[b]School of Information Technology and Engineering,VIT University,Vellore-632014,India

## Abstract

This paper presents a low power modulo $2^n$+1 multiplier in which one input and output uses the weighted representation while the other input uses the diminished-1 representation. The low power in the multiplier is achieved by reducing the number of transition or transition frequency in the adder tree which is used to reduce the partial product and data aware properties is achieved with the help of the master and slave latches, dynamic range detection unit and the bit restoration unit. The dynamic range detection unit detects the dynamic range between the input data's and it allows only those data for the further processing in the adder unit and bit restoration unit take care of the data bit which is lost during the addition. The multiplier proposed in this paper form only n/2 (n=number of input bits)partialproduct which is less than all the partial products produced by the available multiplier. Although by applying this logic there is a area overhead but there is a increase in power saving from 32% to 77% as the number of bits in the input of the multiplier increases from 4 to 32 bit.

*Keywords:*Low power; Adder tree;Master and Slave latch;

## 1. INTRODUCTION

The modulo $\mathbf{2^n}$+1multiplier is the basic block in the design of the residue number system (RNS) filter[6] and international data encryption algorithm (IDEA). So to make it fast and power efficient we have to speed up the multiplier and reduce the power consumption which can be done by decreasing the number of partial product and

doi:10.1016/j.procs.2015.10.033

the transition frequency of the multiplier. Many architectures of the modulo $\mathbf{2^n}$+1 multiplier were proposed earlier. The modulo $\mathbf{2^n}$+1 multiplier proposed by R. zimmermann uses booth encoding but had not taken the advantages of the diminished-1 arithmetic which causes complex architecture[8]. L.sousa et al. modified the radix-4 booth encoding scheme to take the advantages of the diminished-1 arithmetic although partial product gets reduced to (n/2+1) but there is complexity in the area requirement due to the correction term generation block[9]. C.efstathiou et al. proposed diminished-1 modulo $\mathbf{2^n}$+1 multiplier without using the booth encoding but there is no any treatment for the zero operand [4,10]. H. T.ergos et al. proposed a modulo $\mathbf{2^n}$+1 multiplier without booth encoding scheme[5]. The data aware low power modulo $\mathbf{2^n+1}$ multiplier proposed in this paper generate the n/2 partial product using the pure radix-4 booth encoding scheme also it has one input and output in weighted representation while the other input is in the diminished-1 representation moreover correction term is also very simple which take care of the zero operand and the zero result also. The partial product reduction is done through the use of proposed inverted end around carry save adder (IECSA) tree and the final product is generated by using the diminished-1 modulo $\mathbf{2^n}$+1 adder[4].To the best of our knowledge the modulo $\mathbf{2^n}$+1 multiplier design in this paper is the first modulo $\mathbf{2^n}$+1multiplier which uses the data aware IECSA.

The master latches latch the input data. Dynamic range detection unit calculate the dynamic range of the input data and generates the control signals for slave latches and bit restoration unit. The slave latches allow only the dynamic range data to pass in the adder tree for the operation while the remaining data remain same which reduces the number of computation and results in the less power consumption.

## 2. BASIC RESIDUE ARITHEMATIC

### *2.1. Diminished-1 Arithmetic*

In residue number system and in the Fermat number transform we have to deal with n+1 bit (n=number of bits) when the modulus is $\mathbf{2^n}$+1 because of the fact that the maximum value allowed in these type of arithmetic is 2n which is represented by n+1 bit. But it does not seems to be good to work with the extra bit so a new approach is introduced which maps the number in the normal weighted binary representation to a modified binary representation which brings down the number into the n bit and this new approach is known as the diminished-1 representation. The diminished-1 representation of binary number was proposed by L. leibowitz, which is a very efficient form for modulo $\mathbf{2^n}$+1operation on the binary number[1]. The diminished-1 representation operation is defined as follow:

$$d[\,-A\,] = d[\,\bar{A}\,], d[\,A\,] \in [0,2^n - 1] \quad (1)$$
$$d[\,A+B\,] = |\,d[A] + d[B] + 1\,|_{2^n+1} \quad (2)$$
$$d[\,A-B\,] = |\,d[A] + d[\bar{B}] + 1\,|_{2^n+1} \quad (3)$$
$$d[\,AB\,] = |\,d[A] \times d[B] + d[A] + d[B]\,|_{2^n+1} \quad (4)$$
$$d[\,2^k A] = iCLS(d[A],k), d[A] \in [0,2^n - 1] \quad (5)$$
$$d[\,-2^k A] = iCLS(d[\bar{A}],k), d[A] \in [0,2^n - 1] \quad (6)$$

Where $d\,[\,\bar{A}\,]$ represent the 1's compliment of d[A].and i CLS(d[A],k) is the k bit left circular shift of d[A] in which the k bits left circulated into the LSB is complemented.

The modulo $2^n$+1 multiplier which use the proposed data aware IECSA is shown in Fig.1.(b) while the modulo $2^n$+1 multiplier proposed by Jian Wen Chen et al. [13]is shown in Fig.1.(a).The multiplier proposed in this paper is consist of the following sub blocks:

1)The partial product generator(PPG) and the correction term generator(CTG).
2)Proposed data aware Inverted End Around Carry Save Adder Tree (IECSA).
3) The Diminished-1 Modulo $2^n$+1 Adder (DMA).

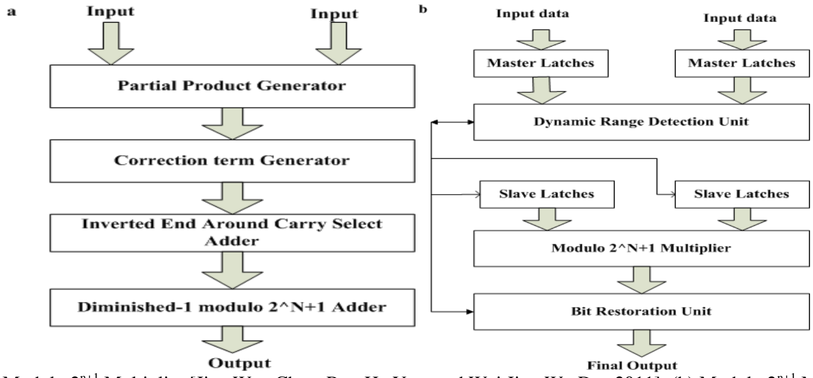
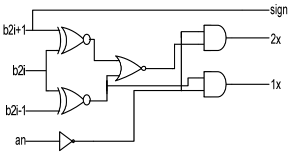

a
Input
Input
Partial Product Generator
Correction term Generator
Inverted End Around Carry Select Adder
Diminished-1 modulo 2^N+1 Adder
Output
b
Input data
Input data
Master Latches
Master Latches
Dynamic Range Detection Unit
Slave Latches
Slave Latches
Modulo 2^N+1 Multiplier
Bit Restoration Unit
Final Output

Fig. 1.(a) Modulo $2^{n+1}$ Multiplier [Jian Wen Chen, Ruo He Yao, and Wei Jing Wu Dec 2011]; (b) Modulo $2^{n+1}$ Multiplier.

### 2.2.1. *Partial Product Generator*

The PPG of the multiplier consist of two block Booth Encoder(BE) and Booth Selector(BS).The function of the BE block is to generate the code while BS block is used to generate the partial product from the encoded output of the BE block. According to the available architecture the BE block can be categories into two groups. Group one and Group two. Group one has a 4-bit bus while Group two have a three- bit bus architecture. The modulo $2^n$+1 multiplier used in this paper uses the Group one BE block having three-bit bus architecture[8].The circuit diagram for the BE block is shown in Fig2.



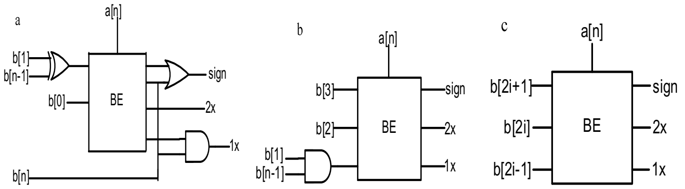


Fig.2.Circuit diagram for BE blockFig.3. (a)BE0 block for n=even; (b) BE1 for n=even; (c) BEi When 1 < i < n/2

The BE blocks of the multiplier examine the successive overlapping triplets$(b_{2i+1},b_{2i},b_{2i-1})_2$and encodes each as an element of the set {-2,-1,0,+1,+2}.Each BE block produces three bit output Sign,2X and1X These three bit along with the multiplicand is used to form the partial product. The Modified BE circuit used to form the three bit output is shown in the Fig.3.(a),Fig.3.(b)and Fig.3.(c).

The BS block take the two successive bit of d[A] as the input. In this multiplier there are two type of BS block $BS^+$ and $BS^-$ since the inverted left circular shift of d[A] and d[-A] are different. The circuit diagram and the truth table for the BS+ and BS- blocks are referred from Jian Wen Chen et al. [13].

The correction term generator produces the vector C which has the form $(\ldots 0x_{i+1}0x_i \ldots 0x_1 0x_0)_2$where $x_i \epsilon \{0,1\}$.Sincethe 2i-th bit $x_i$ is 1 when the$BE_i$blocks encodes 0 otherwise $x_i$ is 0 one XNOR gate accepting the 1x,2x bit of $BE_i$block can generate the 2i-th bit of $x_i$.The IECSA tree in this multiplier is constructed using the proposed data aware adder which uses the low power technique proposed by Oscal T et al [12].While the final adder uses the diminished-1 modulo $2^n$+1 adder since this adder outperform the normal adder in area and delay. The multiplier design in this paper uses the fastest diminished-1 modulo $2^n$+1adder [4].

## 3. Proposed Data Aware Inverted End Around Carry Select Adder Tree

The IECSA tree is in this paper is constructed using the full adder and half adder and it uses the low power technique proposed by Oscal T et al [12]. Fig.6 shows the proposed IECSA tree used in the multiplier of this paper.Since the switching power in digital logic design is given by the equation

$$P_{switching} = \alpha CVDD^2 f_{clk} \quad (7)$$

Where$\alpha$ =Switching activity; C=load capacitance; VDD=operating voltage; $f_{clk}$= operating frequency.

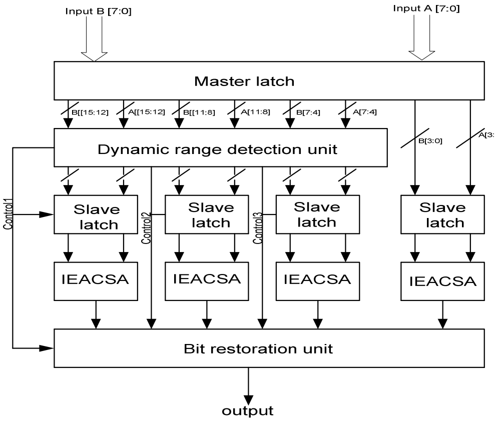


Fig.4.Block diagram of proposed data aware IECSA for 8 bit input data

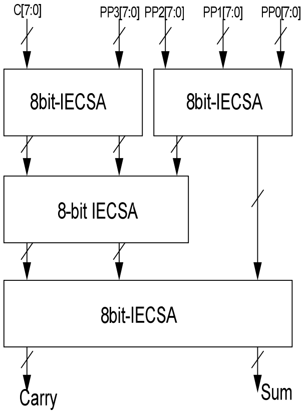


Fig.5. Block diagram of conventional IECSA

From eqn. 7) it is clear that we can reduce the power of the system by the three ways as given below:

- By reducing the supply voltage.
- By reducing the clock frequency.
- By reducing the effective load capacitance. ($\alpha C$)

But the reduction of power in a system by varying the first two parameter also results in the reduction of performance of the system. So the best option to reduce the power is by reducing the effective load capacitance. In this paper we have reduces the power of the modulo $2^n$+1 multiplier by reducing the effective load capacitance of the adder tree so that the performance of the multiplier would not reduce.Fig.5 shows the conventional 8-bit adder tree used in the modulo $2^n$+1multiplier [13]·while Fig.4 shows the proposed data aware low power IECSA adder tree.

In Fig.5 the input data each having the length of 8-bit is directly processed in the adder tree unit without taking care of the relation between input data and output result. If the effective dynamic range of the input data is 4 bit then the first 4MSB bits of the input data have no significance and thus is wasteful in the overall operation.

For example: if we have A=1111_1010 and B=1111_0001 as the input to the adder tree then the sum and carry separately is given by sum=0000_1011 and carry =1110_0000.It is clear therefore that the first 4 bit of MSBof sum do not affect the adder result so we can save the unnecessary transition at the node of the multiplier. Suppose if the present output of the adder tree is zero and the previous output of the adder is one but due to the dynamic range the present output has no any effect on the sum results so these bit can remain in the previous state and several unnecessary from 1 to 0 or vice-versa can be prevented.

Following are the main block of the data aware proposed adder which is used in the modulo $2^n$+1 multiplier in this paper.

- Master latches
- Dynamic range detection unit
- Slaves latches
- Adder unit
- A word length restoration unit

The master latch latches the input data while the dynamic range detection unit detects the effective value of the dynamic range of the input data present in the master latches to latch only the data of the effective dynamic range in slaves latch while rest of the data remain in the same state which reduces the unnecessary switching activity in the adder. When the input data are sent to and latched at the master latches, the dynamic range detection unit first checks the effective dynamic range of the input data output from the master latches and generate the control signals and in response to this control signal slaves latch determine whether to hold or pass the bit corresponding to the inputs data. Those bit corresponding to the ineffective dynamic range will be held whereas the bit of the effective dynamic range will be passed. Therefore the adder will not perform operation on the bits corresponding to the ineffective dynamic range while parts corresponding to this bit will not have switching and will remain there at the previous bit. Thus power consumption due to the state switching Frequency and the charge discharge of the capacitor nodes associated with these bits will be significantly reduced. Final output is rebuilt by the word length restoration unit in accordance with the sign and the value of the adder results using the control signals Fig.7.(a) to Fig.7.(e) show the hardware required to implement data aware adder and the Fig.6shows the proposed modulo $2^8$+1multiplier which uses the proposed data aware IECSA in the adder tree.

Hardware Descriptive Language (HDL) and the multiplier description is mapped to45nm CMOS standard cell library (TSMC) using RC compiler tool from cadence. The synthesized Verilog Netlist and their respective design constraints file (SDC) are imported to Cadence SoC Encounter and are used to generate automated layout from standard cells and placement and routing. For each word size of the multiplier the same Value Changed Dump (VCD) file is generated for all possible input condition and imported the same to Cadence Encounter. The similar design flow is followed for the proposed multiplier and the multiplier proposed by Jian Wen Chen et al. [11,13]which is efficient of all the available modulo$2^n$+1 multiplier architecture. To get the more accurate result for the comparison first we have written the Verilog code of the multiplier proposed by Jian Wen Chen et al. [13]and have done the simulation and after that keeping all the constraints same simulation is done for the proposed low power modulo$2^n$+1.Table I and Table II shows the experimental results for area, delay and power for the proposed modulo $2^n$+1 multiplier and the multiplier proposed in [13].

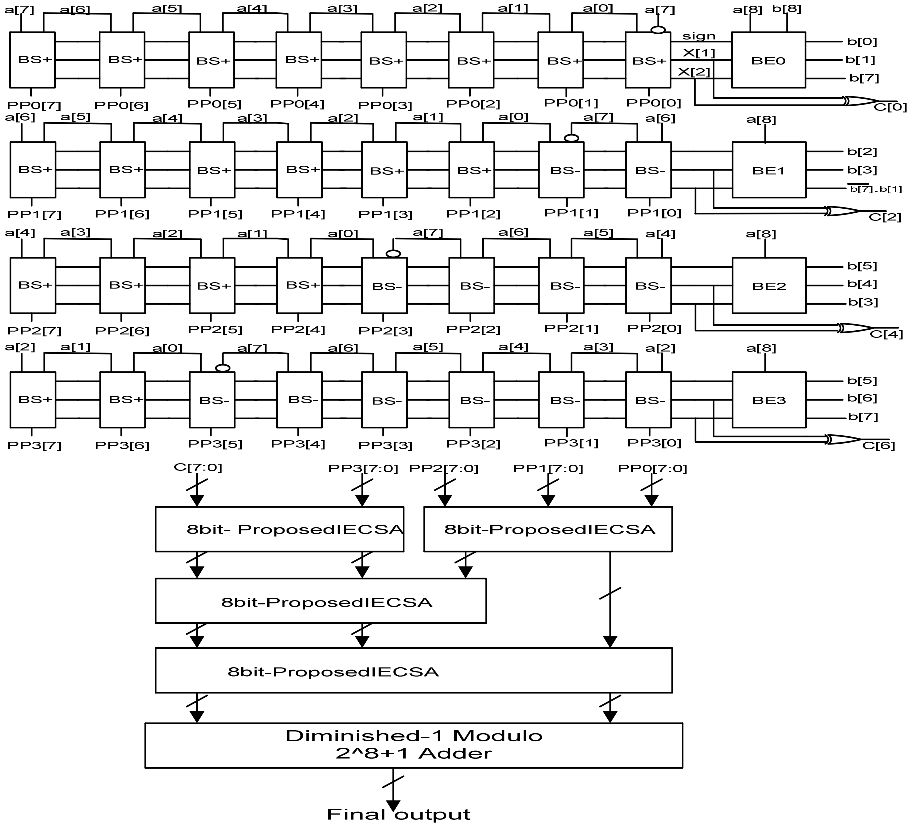

a[7] a[6] a[5] a[4] a[3] a[2] a[1] a[0] a[7] a[8] b[8]
BS+ BS+ BS+ BS+ BS+ BS+ BS+ BS+
sign
X[1]
X[2]
BE0
b[0]
b[1]
b[7]
PP0[7] PP0[6] PP0[5] PP0[4] PP0[3] PP0[2] PP0[1] PP0[0]
C[0]
a[6] a[5] a[4] a[3] a[2] a[1] a[0] a[7] a[6] a[8]
BS+ BS+ BS+ BS+ BS+ BS+ BS- BS-
BE1
b[2]
b[3]
b[7]-b[1]
PP1[7] PP1[6] PP1[5] PP1[4] PP1[3] PP1[2] PP1[1] PP1[0]
C[2]
a[4] a[3] a[2] a[1] a[0] a[7] a[6] a[5] a[4] a[8]
BS+ BS+ BS+ BS+ BS- BS- BS- BS-
BE2
b[5]
b[4]
b[3]
PP2[7] PP2[6] PP2[5] PP2[4] PP2[3] PP2[2] PP2[1] PP2[0]
C[4]
a[2] a[1] a[0] a[7] a[6] a[5] a[4] a[3] a[2] a[8]
BS+ BS+ BS- BS- BS- BS- BS- BS-
BE3
b[5]
b[6]
b[7]
PP3[7] PP3[6] PP3[5] PP3[4] PP3[3] PP3[2] PP3[1] PP3[0]
C[6]
C[7:0]
PP3[7:0] PP2[7:0] PP1[7:0] PP0[7:0]
8bit- ProposedIECSA
8bit-ProposedIECSA
8bit-ProposedIECSA
8bit-ProposedIECSA
Diminished-1 Modulo
2^8+1 Adder
Final output

fig. 6. Block diagram of the proposed modulo 2^8+1 multiplier using proposed data aware IECSA.

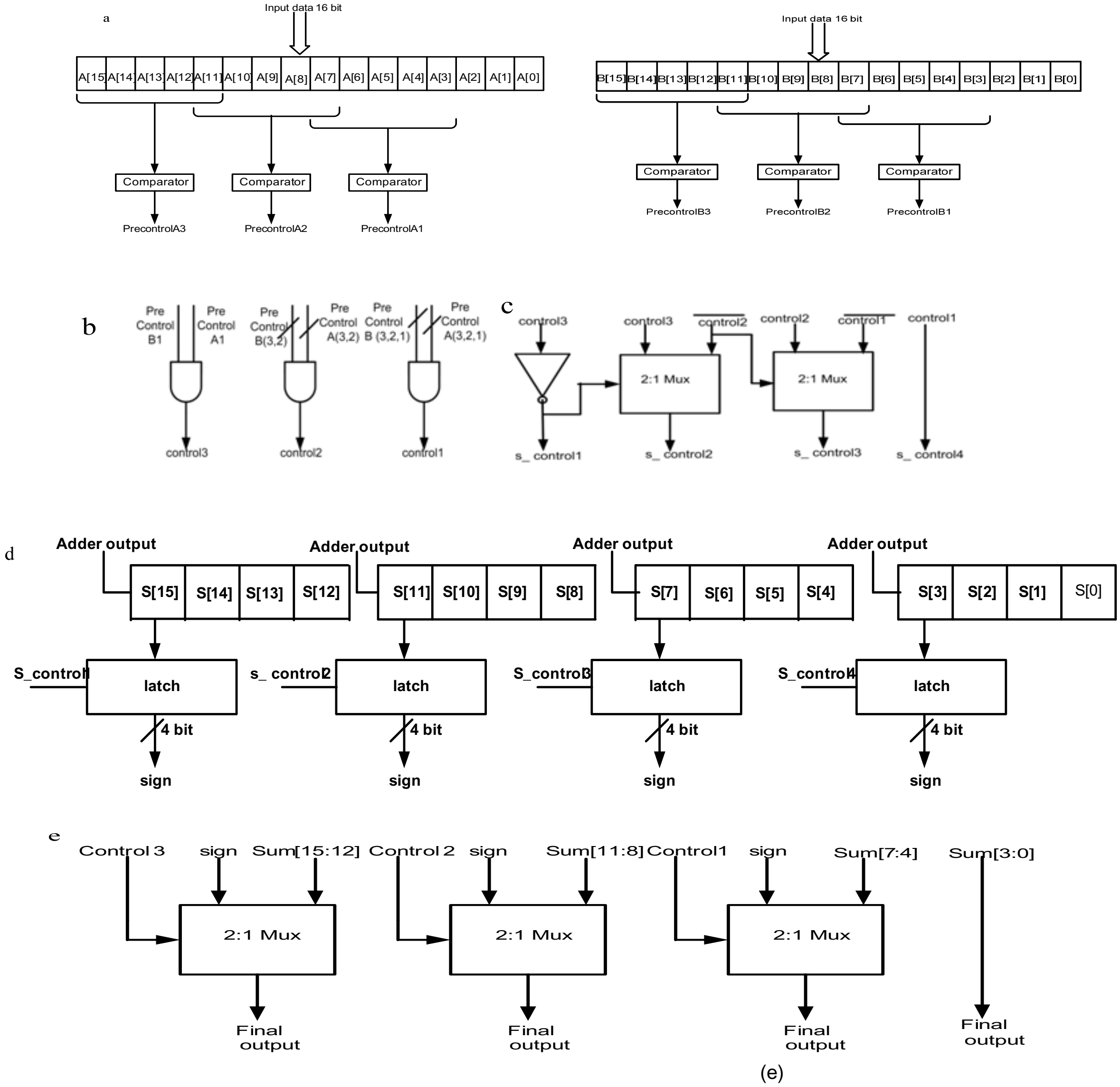


Fig 7. (a) Comparator and master latch; (b) Control signal for dynamic range detection; (c) Sign signal control generator; (d) Sign signal generator; (e) Bit restoration sign unit

Table I: Experimental results showing area, %age area overhead and delay of the modulo $2^n$+1multiplier with and without proposed adder

| No of bits | A1($\mu$m$^2$)* | A2($\mu$m$^2$)# | Area Overhead (%) | Delay1(ps) | Delay2(ps) | Delay Overhead(%) |
|---|---|---|---|---|---|---|
| 4 | 329.337 | 446.549 | 35% | 3690 | 4520 | 22.5 |
| 8 | 1410.450 | 1851.074 | 31% | 6456 | 6960 | 18 |
| 16 | 5388.340 | 6686.875 | 24% | 8889 | 10517 | 7.8 |
| 32 | 30494.459 | 32220.548 | 5% | 12100 | 12100 | 0 |

*Area of multiplier without data aware IECSA
#Area of multiplier with proposed data aware IECSA
Delay1is delay of multiplier without data aware IECSA
Delay2is delay of multiplier with proposed data aware IECSA

TableII: Experimental results showing power of modulo $2^n$+1 multiplier with and without the proposed adder

| No of bits | P1(nw)* | P2(nw)# | Power Saving (%) | Power Delay Product($10^{13}$) (Old) | Power Delay Product($10^{13}$) (Proposed) | Power Delay Product reduction (%) |
|---|---|---|---|---|---|---|
| 4 | 19231.585 | 25371.689 | 32% | 0.7 | 1.14 | -62.85 |
| 8 | 125129.992 | 95333.443 | 31% | 8.07 | 6.63 | 17 |
| 16 | 466043.268 | 311948.253 | 49% | 40.142 | 3.28 | 24 |
| 32 | 2598192.926 | 1460287.218 | 77% | 300.143 | 1.76 | 66 |

*Power consumed by multiplier without data aware IECSA

*Power consumed by multiplier with data aware IECSA

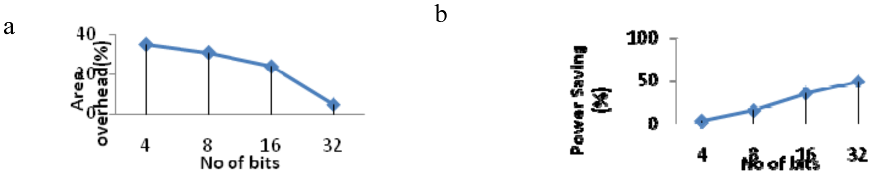


Fig.8. (a)Graph of area overhead of new multiplier over the multiplier proposed in [Jian Wen Chen, Ruo He Yao, and Wei Jing Wu, Dec, 2011]with the variation of bits from 4 to 32; (b) Graph of power saving of proposed multiplier over the multiplier proposed in[Jian Wen Chen, Ruo He Yao, and Wei Jing Wu, Dec, 2011] with the variation of no. of bits from 4 to 32

## 4. conclusions

In this paperlow power modulo $2^n$+1 multiplier using data aware adder tree is proposed. The proposed low power modulo multiplier $2^n$+1 consist of the master and slaves latches, dynamic range detection unit, radix-4 booth encoder, proposed inverted end around carry select adder tree,diminished-1 modulo adder and bit restoration unit. The multiplier proposed are designed for various lengths of the input data and simulated to generate the results. The results shows that the proposed data aware low power modulo$2^n$+1 multiplier has low power but area overhead of 35% ,31%,24% and 5% for n= 4,8,16.32 respectively which is decreasing with the increase in the number of bits so for the higher number of bits area overhead can be neglected.

## References

1. Leibowitz L. A simplified binary arithmetic for the Fermat number transform', IEEE Trans. Acoust. Speech Signal Process.,(1976), ASSP-24,,(1976), pp. 356–359.
2. L. Sousa and R. Chaves. A universal architecture for designing efficient Modulo $2^n$ +1multipliers *IEEE Trans. Circuits Syst. I, Reg.Papers*,vol. 52, no. 6, ( Jun. 2005) pp. 1166–1178 .
3. C. Efstathiou,H. T.Vergos,G. Dimitrakopoulos, and D.Nikolos, Efficient diminished-1 modulo $2^n$+1multipliers,*IEEE Trans. Comput*.vol. 54, no. 4, (Apr. 2005) pp. 491–496.
4. H. T. Vergos, C. Efstathiou, and D. Nikolos, "Diminished-one modulo$2^n$+1 adder design," *IEEE Trans. Comput.*, vol. 51, no. 12, (Dec. 2002) pp.1389–1399.
5. H. T. Vergos and C. Efstathiou, "Design of efficient modulo $2^n$+1multipliers," *IET Comput.Digit.Tech.*, vol.1, no.1, Dec. (2002) pp. 49–57, 2007.
6. Conway R, Nelson J. Improved RNS FIR filter architectures, IEEE Trans. Circuits and Systems. II, EXP.Briefs(2004)51,(1),pp. 26-28
7. W. C. Yeh and C. W. Jen, "High-speed booth encoded parallel multiplierdesign," *IEEE Trans. Comput.*, vol. 7, pp. 692–701, 2000.
8. R. Zimmermann,Efficient VLSI implementation of modulo $2^n$+1 addition and multiplication, in *Proc. 14th IEEE Symp. Comput.Arithm.*, Adelaide, Australia, Apr.(1999), pp. 158–167.
9. L. Sousa and R. Chaves, A universal architecture for designing efficient Modulo$2^n$+1 multipliers, *IEEE Trans. Circuits Syst. I, Reg.Papers*, vol. 52, no. 6,Jun. 2005 pp. 1166–1178.
10. C. Efstathiou,H. T.Vergos,G. Dimitrakopoulos, and D.Nikolos, Efficient diminished-1 modulo $2^n$+1 multipliers,*IEEE Trans. Comput.*,vol. 54, no. 4,(Apr. 2005) pp. 491–496.
11. J.W. Chen and R.H. Yao. Efficient modulo 2n + 1 multipliers for diminished-1 representation. Circuits, Devices Systems, IET, 4(4):291 -300, (jul. 2010).
12. OscalT I-Ping Hsu, Ruey-Liang Ma, "Arithmetic device and method with low power consumption" US Patent 2003 Patent No: US 6,629,119 .
13. Jian Wen Chen ,Ruo He Yao,Wei Jing Wu, "Efficient modulo 2n + 1 multipliers", *IEEE Transt on V.L.S.I.*,vol. 19, no. 12,(Dec. 2011) .