International Journal of Engineering & Technology, 7 (4.20) (2018) 31-35

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research paper

Diminished-1 multiplier using modulo $2^n + 1$ adder

Beerendra Kumar Patel[1*], **Jitendra Kanungo**[2]

[1*] *Department of Electronics &Communication Engineering*
[2]*Jaypee University of Engineering &Technology, Guna (M.P.), India*
**Corresponding author E-mail:*beerendrapatel23@gmail.com

Abstract

In this work Modulo multiplier offers higher computational speed than a normal multiplier. It is frequently used in data security and residue number system. The modulo$2^n + 1$ has three basic blocks-partial product generation block, inverted end around carry adder tree block and diminished-1 modulo$2^n + 1$ adder block. The result and an operand use weighted representation and others uses the diminished-1 for the modulo multiplier. The multipliers receive full inputs and avoid (n+1) bits circuits due to diminished-1 number representation. In this work, proposed modulo $2^n + 1$ multiplier with modified diminished-1 modulo$2^n + 1$ adder which is based on ripple carry adder. The proposed design saves significant area and power as compared to the reported one with little increment in delay.

Keywords: *Residue number system, computer arithmetic, diminished-1 representation, modulo* $2^n + 1$ *adders.*

1. Introduction

Modular arithmetic is a system of arithmetic of numbers where numbers are "warp around" upon reaching a certain values. A new number system arises called as Residue Number System (RNS) from the modular arithmetic. RNS represents higher arithmetic numbers into smaller arithmetic number, so that performance of computation more efficiently. The RNS [1] residues the delay of carry propagation, that makes suitable for the implementation of high speed digital signal processing devices. Some arithmetic operation, such as addition and multiplication can be carried out more efficiently in RNS than in conventional two's complement method. RNS has been adopted in the design of Digital signal processors, Finite impulse response filter, image processing units, discrete cosine transform processors, communication components and others DSP applications [2].

Modulo $2^n + 1$ multiplier has been used in wide range of applications including random number generators which has remarkable applications in communication system and in cryptographic algorithms [3] used for transmission of the data. Various cryptographic systems have been studied and implemented to ensure the security of these systems [3].

International Data Encryption Algorithm (IDEA)[3] is most reliable cryptographic algorithm used for communication of the data. The three major operations that decide the delay and the overall performance of IDEA cipher are modulo 2^n addition, bitwise-XOR and modulo $2^n + 1$ multiplication, in the hardware implementation. The performance of data path of the IDEA cipher essentially depends on the modulo $2^n + 1$ multiplication.

Apart from this, the modulo $2^n + 1$ module has found in applications such as digital signal processing and fault tolerant design of ad-hoc networks [4]. Pseudorandom number generation is the special case of the linear congruential sequence which uses modulo$2^n + 1$ multiplication to obtain a long sequence of pseudorandom numbers. Rest of the paper is organized as follows. The arithmetic for diminished-1 representation is briefly introduced in section II. In section III, the modular multiplication architecture is derived. In section IV, diminished-1 Modulo $2^n + 1$ Adder Module is introduced. The simulation result is discuss section V.

2. Mathematical equation and problem formulation

In modulo $2^n + 1$ multiplication, one input uses weighted representations and other input uses diminished-1 representation.

Let D[α]=(α_n,α_{n-1}……..α_0) be the diminished-1 representation of the weighted binary number A,B =(β_n, β_{n-1}……..β_0) and P =$|\alpha \times \beta|_{2^n+1}$ all be weighted binary numbers, The algorithm uses D[α] and β to compute the value of P, that is

$$P = (\alpha \times \beta) \bmod (2^n + 1) = |\alpha \times \beta|_{2^n+1} = F(D[\alpha], \beta) \quad (1)$$

The modulo $2^n + 1$ multipliers can be used for the situation where one operand being constant and another operand being varied. So the diminished-1 representation of the constant operand and can be pre-computed and be preset in the hardware, so its conversion circuits are not required.

The algorithm uses the radix-4 Booth recoding [11], where successive overlapping triplets of B are examined and encoded. The outputs of the encoder use the D[α] to form the partial products. The partial product reduction scheme uses the well known Inverted End Around Carry (IEAC) adder tree [11]. The final adder generates the product. To avoid (N+1)-bit circuits, there be two cases when $\overline{\alpha_n + \beta_n}$=1 and when $\overline{\alpha_n + \beta_n} = 0$

A. When $\overline{\alpha_n + \beta_n}$=1
In this case, α_n=0 and b_n=0

$$\beta = \sum_{j=0}^{n-1} b_j 2^j$$

$$= \left| b_0 - 2b_1 + \sum_{i=1}^{[n/2]} (b_{2i-1} + b_{2i} - 2b_{2i+1}) 2^{2i} \right|_{2^n+1} \quad (2)$$

When, n is even, B can be expressed as (2), because $b_{n+1} = b_n = 0$ and $\left|2^n\right|_{2^n+1} = \left|-1\right|_{2^n+1}$, we get

$$\beta = \left| \begin{matrix} b_0 - 2b_1 + (b_{n-1} + b_n - 2b_{n+1})2^n + \\ \sum_{i=1}^{[n/2-1]} (b_{2i-1} + b_{2i} - 2b_{2i+1}) 2^{2i} \end{matrix} \right|_{2^n+1} \quad (3)$$

$$= \left| \begin{matrix} -b_{n-1} + b_0 - 2b_1 + \\ \sum_{i=1}^{[n/2-1]} (b_{2i-1} + b_{2i} - 2b_{2i+1}) 2^{2i} \end{matrix} \right|_{2^n+1} \quad (4)$$

It is obvious that $b_{2i-1} + b_{2i} - 2b_{2i+1}$ corresponds with the radix-4 Booth recoding scheme, but $-b_{n-1} + b_0 - 2b_1$ does not. There exists a "hard multiple" -3 for $-b_{n-1} + b_0 - 2b_1$ when .To eliminate this "hard multiple", we have two cases: (1) when $b_{n-1} = 1$ and (2) $b_{n-1} = 0$, In equation(4)

$$\beta = \left| \begin{matrix} (b_{n-1} + b_0 - 2(b_{n-1} \oplus b_1) + (b_1 . \overline{b_{n-1}} + b_2 - 2b_3) 2^2 \\ + \sum_{i=2}^{[n/2-1]} (b_{2i-1} + b_{2i} - 2b_{2i+1}) 2^{2i} \end{matrix} \right|_{2^n+1} \quad (5)$$

In equation (5) all corresponds with the radix-4 booth recoding scheme, and their values may be equal to $0, \pm 1, \pm 2$ .To make this

$$\begin{aligned} E_0 &= b_{n-1} + b_0 - 2(b_{n-1} \oplus b_1 \\ E_1 &= b_1 . \overline{b_{n-1}} + b_2 - 2b_3 \\ E_i &= b_{2i-1} + b_{2i} - 2b_{2i+1} \end{aligned} \quad (6)$$

When (5) can be expressed as when n is even

$$\beta = \left| E_0 2^0 + E_1 2^2 + \sum_{i=2}^{[n/2-1]} E_i 2^{2i} \right|_{2^n+1}$$

$$\beta = \left| \sum_{i=0}^{[n/2-1]} E_i 2^{2i} \right|_{2^n+1} \quad (7)$$

In a similar way, when B can be odd as

$$\beta = \left| \sum_{i=0}^{[n+1/2-1]} E_i 2^{2i} \right|_{2^n+1} \quad (8)$$

$$P = \left| \alpha \times \beta \right|_{2^n+1}$$

$$P = \left| d[\alpha \times \beta] + 1 \right|_{2^n+1} = \left| d[\alpha] \times \beta + \beta \right|_{2^n+1} \quad (9)$$

$$d[\alpha.\beta] = \left| \sum_{i=0}^{k-1} pp_i + \sum_{i=0}^{k-1} c_i + k \right|_{2^n+1}$$

From literature survey [5]-[11], we found that the operands and the reduction of partial products are most important factor for the designing of modulo $2^n + 1$ multiplier and also in the final stage adder. The modulo $2^n + 1$ has four basic block:- partial products generation block, inverted end around carry save adder tree block and a modulo $2^n + 1$ adder block. In some papers [4-6], the decrease the number of partial products gives better compact area and some were focused on the operand .But, all the existing architectures have used the final stage modulo $2^n + 1$ adder. Final stage adder become diminished-1 modulo $2^n + 1$ adder by using diminished-1 operand this offers large area and power consumption to the modulo $2^n + 1$ multiplier. Hence, an optimized design of modulo adder is also important.

We have to consider the followings to design low power and area efficient modulo $2^n + 1$ multiplier -

i) One operand in diminished-1 number representation.
ii) Technique for the reduction of number of partial products.
iii) A diminished-1 modulo 2n+1 adder which consumes less power and area.

Therefore design of efficient modulo $2^n + 1$ multiplier it is necessary to get an efficient diminished-1 modulo $2^n + 1$ adder. In this work low power area efficient modulo $2^n + 1$ multiplier with an efficient diminished-1 modulo $2^n + 1$ ripple carry adder.

3. Architecture of Modulo $2^n + 1$ Multiplier

The modulo $2^n + 1$ has three basic blocks: partial products generation block, inverted end around carry adder tree block and diminished-1 modulo $2^n + 1$ adder block which is shown in fig -1

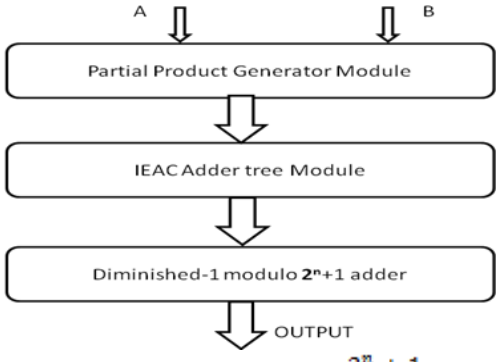

Fig:1. Architecture of modulo $2^n + 1$ multiplier

3.1 Partial Product Generation Module

A standard approach that might be taken by a novice to perform multiplication is the "shift and add", or normal "long multiplication". That is, for each column in the multiplier, shift the multiplicand the appropriate number of columns and multiply it by the value of the digit in that column of the multiplier, to obtain a partial product . The partial product are then added to obtain the final results as shown below

```
  001011
  010011
  001011
 001011
000000
000000
001011
001101000 1
```

With this method, the number of partial products is exactly the number of bits in the multiplier term.
Booth multiplication [5] is a technique that allows smaller, faster multiplication circuits. It is the standard technique used in chip design and provides significant improvements over the "long multiplication" technique. There are several booth recoding scheme present among which radix-4 booth recoding is best one which reduces the number of partial products into n/2 for n even and (n+1)/2 for n odd.

3.2 The IEAC Adder Tree Module

The partial products of n bits and the correction term are added through inverted end around carry (IEAC) adder tree. The total numbers of partial products are generated as K and one correction term. The IEAC adder tree is usually constructed with full adder (FA) and each full adder is constructed by two Half Adders (HA). The K+1operands are added and converted to two numbers. The addition of the K+1 operands are shown in fig.2 and the structure of n bit IEAC adder is also shown (n=8).

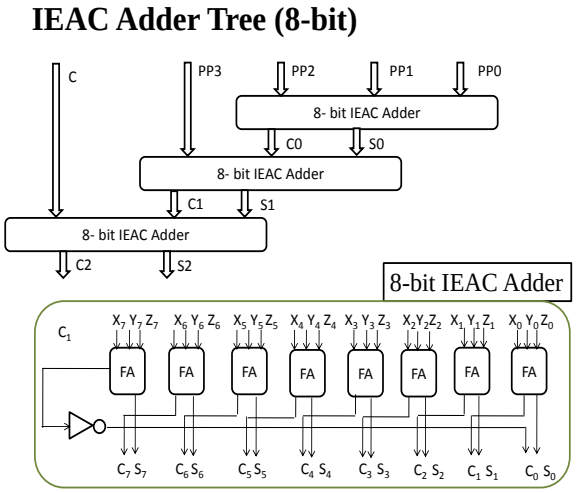

Fig. 2: (a) IEAC Adder Tree (n=8) and (b) 8-bit inverted end around carry adder (n=8)

The n-bit IEAC adder takes three n-bit operands and give a result of sum and carry which are also n-bit as shown in figure3. The CC_0,CC_1,CC_2,CC_3 are the intermediate carries of length 'n' and SS_0,SS_1,SS_2,SS_3 are the intermediate sums of length 'n'.
One correction term and partial product terms are generated For n=16. These are added through the IEAC adder tree which is shown in figure3

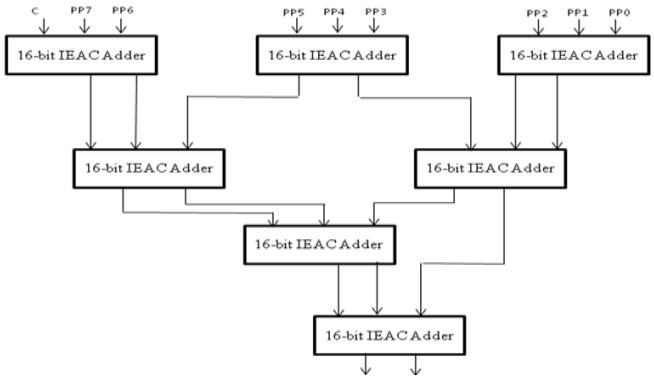

Fig.3: IEAC Adder Tree for (n=16)

4. Proposed diminished-1 Modulo $2^n + 1$ Adder Module

The output of the IEAC adder tree is finally added through a diminished-1 modulo $2^n + 1$ adder. The expression for diminished-1 modulo $2^n + 1$ adder is

$$S^* \bmod(2^n+1) = \begin{cases} (x^*+y^*) \bmod 2^n, if \ldots x^*+y^* \geq 2^n \\ x^*+y^*, otherwise \end{cases}$$

Where S*, x* and y* are the diminished-1 representation of S, x and y respectively. S is the sum of x and y.This expression revels that a diminished-1 modulo adder can be implemented by incrementing the sum by one when the carry output is zero. This can be achieved by connecting the carry output via an inverter back to the carry input. Therefore we can take that the diminished-1 addition is a two cycle operation.
1st cycle: During this addition the input carry is 1.
2nd cycle: During this addition the input carry is 1.
Example 1:- Consider Diminished-1 modulo 9 addition of L=4 with M = 7 and N=3. Then we have $L^*=011_2$, $M^*=110_2$ and $N^*=011_2$.
$L^*=011_2$ $L^*=011_2$
$M^*=110_2$ $N^*=011_2$

```
L* = 011
M*= 110
  1001  > 2³
    ↘ 0
    001
        → Correct result
```

```
L* = 011
N* = 011
  0101 < 2³
    ↘ 1
    110
        → Correct result
```

The structure of the proposed diminished-1 modulo $2^n + 1$ adder is shown in figures. It takes two n-bit operands that are generated from the IEAC adder

tree.

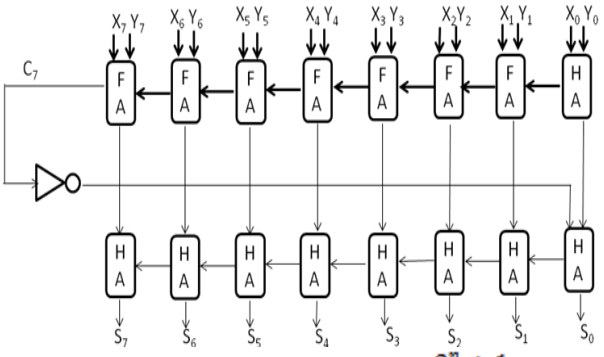

Fig.4: Proposed diminished-1 modulo $2^n + 1$ adder

Example 2:- consider modulo $2^8 + 1$ multiplier with input α = $(227)_{10}$, β =$(157)_{10}$ So D[α] = $(226)_{10}$, = $(11100010)_2$,and the result P = $|\alpha \times \beta|_{2^8+1}$ =$(173)_{10}$ D[α] and β is the input to the multiplier.

N=8, D[α] = $(11100010)_2$, β =$(10011101)_2$, , $\alpha_8 = 0$, $\beta_8 = 0$

Partial products and the correction term are generated as from table 2 to table 5

Encode		Partial Products	
($\beta_8$or($\beta_7$xorβ_1)) β_0 (β_7 or β_1)	011	PP_0	11111111
β_3 β_2 β_1 (not β_7)	110	PP_1	01110111
β_5 β_4 β_3	011	PP_2	01000011
β_7 β_6 β_5.	100	PP_3	11110001
		C = 00000001	

The partial products and the correction term are added through IEAC adder tree and finally through the proposed diminished-1 modulo adder given in following figure-6

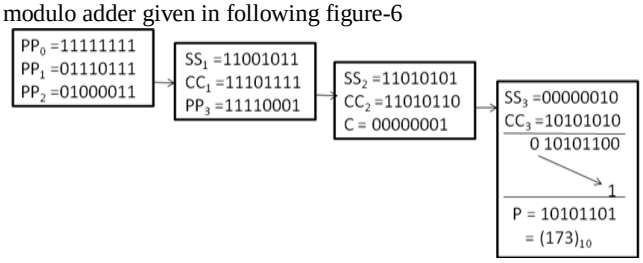

Fig. 5: IEAC Adder Tree.

Table 1: Comparison of simulation result of diminished-1 modulo $2^n + 1$ adders

Gate	8 bit(n=8)		12 bit(n=12)		16 bit(n=16)	
	Jien et al.[11]	Proposed	Jien et al.[11]	Proposed	Jien et al.[11]	Proposed
XOR	16	23	24	35	32	47
AND	64	23	104	35	144	47
OR	40	7	64	11	88	15
NOT	1	1	1	1	1	1

Table-2: Comparison of simulation result of diminished-1 modulo $2^n + 1$ adders

Gate	8 bit(n=8)		12 bit(n=12)		16 bit(n=16)	
	Jien et al.[11]	Pro-posed	Jien et al.[11]	Pro-posed	Jien et al.[11]	Pro-posed
Area	1269.84	602.41	1921.07	95.91	2775.03	1491.38
Pow-er	1.115	0.838	1.733	1.263	2.346	1.678
Delay	8	9	9	12	10	14

Table-3:- Comparison of simulation result of diminished-1 modulo $2^n + 1$ adders

Gate	8 bit(n=8)		12 bit(n=12)		16 bit(n=16)	
	Jien et al.[11]	Pro-posed	Jien et al.[11]	Pro-posed	Jien et al.[11]	Proposed
Area	4901.52	4255.26	9127.57	8389.34	15370.1	14436.714
Pow-er	14.281	12.751	16.256	14.716	30.077	28.503
Delay	15	16	16	19	19	22

With the theoretical comparison, it is clear that the proposed diminished-1 modulo $2^n + 1$ adder has less number of basic gates as compared to the existing one [11]. From Table 2, it is clear that the proposed adder consumes less power and more it is compact with a little bit increase in delay. Hence the use of the proposed diminished-1 modulo $2^n + 1$ adder, the power and area of modulo $2^n + 1$ multiplier have been reduced as shown in the Table 3.

4. Conclusion

In this work, low power and area efficient modulo $2^n + 1$ multiplier has been proposed by using the proposed diminished-1 modulo $2^n + 1$ adder. One operand of the multiplier is used as diminished-1 while the other operand and the result used weighted one. For reducing the number of partial products radix-4 booth recoding [11] is used so that the numbers of partial products are reduced to n/2 for n even and (n+1)/2 for n odd. "by using one operand as diminished-1," the correction term generator circuit being simpler. The partial products and the correction term are added through IEAC adder tree and finally added through proposed diminished-1 modulo $2^n + 1$ adder. The theoretical and simulation results indicate that the proposed architecture consumes less power and it is more compact. But, the cost we have to pay is the delay.

In the proposed architecture, if we apply the modified radix-4 booth recoding technique then the delay may be reduced and the performance of the architecture may efficient.

References

[1] P. V. A. Mohan,Residue Number Systems*: Algorithms and Architectures*, Norwell, MA: Kluwer(2002).

[2] R. Zimmermann, A. Curiger, H. Bonnenberg, H. Kaeslin, N. Felber, and W. Fichtner, "A 177 Mb/s VLSI implementation of the International Data Encryption Algorithm," *IEEE J. Solid-State Circuits*, vol. 29, no. 3, pp. 303–307(1994).

[3] J. Ramirez, A. Garcia, S. Lopez-Buedo, and A. Lloris "RNS Enabled digital signal processing", *Electronics Letters*, vol. 38, no. 6, pp. 226-268,(2002)

[4] Y. Kong and Braden, "Fast scaling in the residue number system," *IEEE Trans. VLSI Syst.*, vol. 17, pp. 443–447(2009).

[5] Curiger, H. Bonnenberg, and H. Kaeslin,"Regular VLSI architecture for multiplication modulo $2^n + 1$,"*IEEE J. solid state circuits*, vol. 26, no. 7, pp. 990-994(1991).

[6] Z. Wang, G. A. Jullien, and W. C. Miller, "An efficient tree architecture for modulo $2^n + 1$ multiplication," *J. VLSI Signal Process. Syst.*, vol. 14, no. 3, pp. 241–248(1996).

[7] R. Zimmermann,"Efficient VLSI implementation of modulo addition and multiplication," in *Proc. 14th IEEE Symp. Comput. Arithm.*, Adelaide, Australia, pp. 158–167(1999).

[8] 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, pp. 1166–1178(2005).

[9] 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, pp. 491–496(2005).

[10] H. T. Vergos and C. Efstathiou , "Design of efficient modulo $2^n + 1$ multipliers," *IET Comput. Digit. Tech.*, vol. 1, no. 1, pp. 49–57(2007).

[11] J.W. Ruo, R. H. Tao and W.J. Wu, "Efficient modulo $2^n + 1$ multiplier,"*IEEE Trans*. VLSI system, Vol.19,No.19(2011).

[12] H. T. Vergos, C. Efstathiou, and D. Nikolos, "Diminished-one modulo $2^n + 1$ adder design," *IEEE Trans. Comput.*, vol. 51, no. 12, pp. 1389–1399(2002).

[13] H. T. Vergos and C. Efstathiou, "A unifying approach for weighted and diminished-1 modulo addition," *IEEE Trans. Circuits Syst. II, Exp. Briefs*, vol. 55, no. 10, pp. 1041–1045(2008).