International Journal of Application or Innovation in Engineering & Management (IJAIEM)
Web Site: www.ijaiem.org Email: editor@ijaiem.org, editorijaiem@gmail.com
Volume 2, Issue 5, May 2013 ISSN 2319 - 4847

Design of Sparse Diminished-1 Modulo (2^n+1) Adder

Denny Oinam[1], K. Saravanan[2], Raja .M[3], Yogaraj .A[4]

[1]Student, Veltech Multitech Dr.Rangarajan Dr.Sakunthala Engg.College, Chennai, Tamil Nadu, India
[2]Assistant Professor, Veltech Multitech Dr.Rangarajan Dr.Sakunthala Engg.College, Chennai, Tamil Nadu, India
[3]Assistant Professor, Veltech Multitech Dr.Rangarajan Dr.Sakunthala Engg.College, Chennai, Tamil Nadu, India
[4]Assistant Professor, Veltech Technical University Chennai, Tamil Nadu, India

ABSTRACT

The parallel prefix adders are area effective and regular due to the parallel-prefix carry operator used. A prefix operator called the gray operator is used to design sparse diminished-1 modulo (2^n+1) adder that leads to implementation in smaller area and consumes less power compared to all earlier proposals and maintains a high operation speed. This adder architecture has a limitation that it is not used for the addition of zero operands. Separate circuit block to handle the zero operand is needed. This makes the design more complex, slow and area-consuming. In order to tackle this issue, a modified modulo adder which can also handle zero operand is developed. This will make it faster and effective. A multiplier is also developed from the modified adder which will be of low power and high speed.

Keywords: Inverted end around carry (IEAC), Modulo arithmetic, Parallel prefix, Sparse.

1 INTRODUCTION

Addition is a fundamental operation for any digital system, digital signal processing or control system. A fast and an accurate operation of a digital system are greatly influenced by performance of the resident adders. The improving performance of the digital adder would greatly advance the execution of binary operations inside a circuit compromised of such blocks. The performance of a digital circuit block is gauged by analyzing its power dissipation, layout area and its operation.

1.1 PARALLEL PREFIX ADDER

Prefix: The output of the system depends on initial input. Parallel: Involves the execution of an operation in parallel. This is done by segmentation into smaller pieces that are computed in parallel. An arbitrary operator "o" that is associative is parallelizable. It is fast because the processing is accomplished in a parallel fashion. Assuming the addition of A= $a_{0,}$ a$1_{........}a_n$ with B = $b_0b_{1............}b_n$ the carry generate term gi, the carry propagate term pi = ai + bi, which can also be defined as pi = hi = ai © bi, where © denotes the exclusive-OR operation

The sum is given by

S = A©B (1)

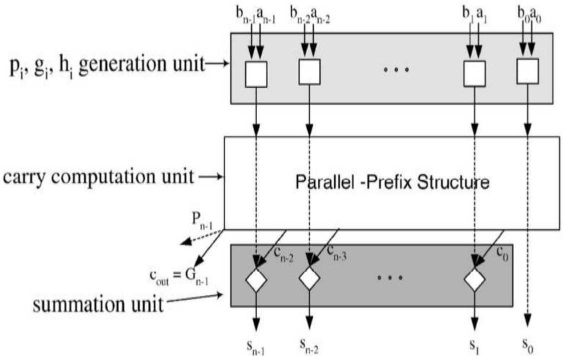


Fig 1: Parallel prefix adder block diagram

1.2 MODULO 2^n+1 ADDER

Let us now discuss modulo 2^n+1 Adder Design. The computation of modulo 2^n+1 addition is in fact a conditional operation defined as

(A+B)Mod (2^n+1) = (A+B), (A+B) <2^n (2)

= (A+B-1) Mod2^n, (A+B) $\geq 2^n$ (3)

There are two main structures of Modulo 2 ^{n} +1 adder. They are structures

- using an additional carry-increment stage
- Reticulating the inverted end around carry within the existing log2 n prefix levels.

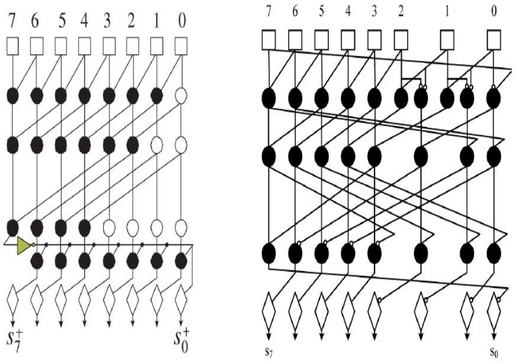


Fig 2: Parallel prefix modulo 2^8+ 1 adders using an additional carry-increment stage and recirculate the inverted end around carry within the existing log2 n prefix levels

1.3 DIMINISHED-1 MODULO 2^N+1 ADDER

The diminished-one number representation is commonly used for modulo 2^n + 1 operation. In this system, the value 0 is treated separately (for example, using an additional zero-indication bit). We will hereafter denote with X* the representation of X in the diminished-one number system, that is, X*=X-1. When none of the input operands is zero, a_z, b_z are not 1, the number part of the diminished-1 sum is derived by the number parts A^* and B* of the input operands as follows:

$$S^*= (A^*+B^*+1) \text{ Mod} 2^n, \quad (A^*+B^*) <2^n \qquad (4)$$
$$= (A^*+B^*) \text{ Mod} 2^n, \quad (A^*+B^*) \geq 2^n \qquad (5)$$

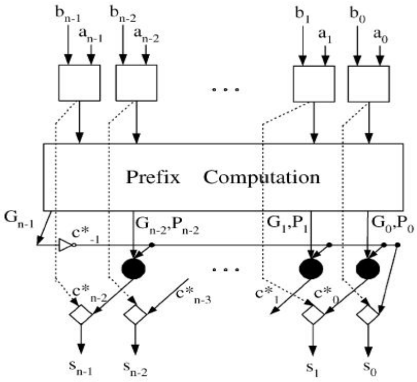


Fig 3: Modulo 2n+1 adder architecture for diminished-one arithmetic

1.4 SPARSE MODULO 2^n+1 ADDERS

Sparse refer to the design of the adder where a carry select block will be used to obtain the output sum. The possible outputs of sum will be calculated and the output carry will select which output sum will be selected. The design is based at parallel-prefix adders. In the sparse carry computation unit for sparse modulo 2^n +1 diminished adders some prefix operators are doubled up, since 2 carry computations need to be performed in parallel; one on normal propagate and generate signals, while the other on their complements. The problem gets worse when the input operands' width is not a power of two. So there is still a lot of space for improvement. This problem is removed by introducing a new prefix operator and an even simpler carry computation unit. While calculating the carry for the spares adder we found that several operators double up since the operators is calculated in parallel. For larger adders, significantly more operators need to be doubled up, leading to increased area and wiring. To overcome this problem, we need a prefix operator that can associate the operation. We introduce a new operator, hereafter called gray operator.

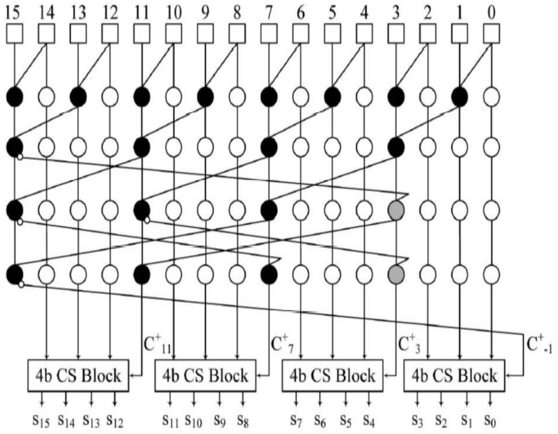


Fig 4: The sparse-4 modulo 2^{16} +1 diminished-1 adder.

The disadvantages of the system are given

- The diminished-1 adder is slower than full parallel prefix architecture.
- Diminished-1 modulo 2^n+1 addition is not used for addition of zero operands. When the input operand is zero, it should be handled separately.
- Zero treatment leads to slow and area-consuming implementations

2. PROPOSED MODULO 2^n+1 ADDER

Architecture of Zero handling unexceptional modulo adders will be designed and the performance evaluation by means of area, delay, power dissipation will be compared with existing modulo adder. The problem of designing an Extra hardware for handling Zero addition problem is recovered in our proposal by implementing a MUX based selection line is used to decide whether to perform addition in case of input zero.

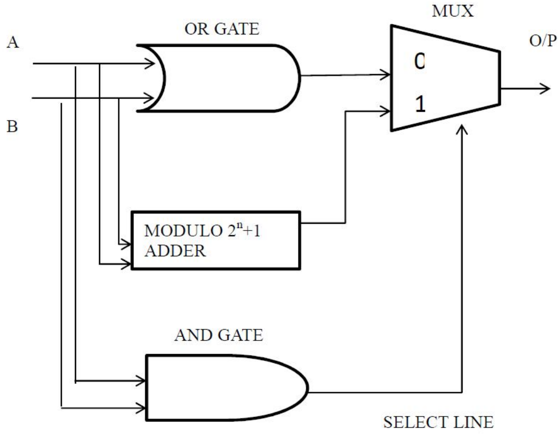


Fig 5: Proposed adder diagram

The operation of the proposed adder is discussed below.

Table 1: Operation of the Proposed Adder

A	B	OR o/p	AND o/p	SELECT	OUTPUT
0	0	0	0	0	0
0	B	B	0	0	B
A	0	A	0	0	A
A	B	-----	AB	1	A+B mod

3. PROPOSED MODULO (2^n+1) MULTIPLIER

By extending the existing adder design a shift modulo multiplier will be designed for working with cryptosystems. The developed multiplier consists of shift and add phase. In shift phase, the product register is shifted left by one digit and the proper multiple of X is added using modulo adder. The modulo adder will produce a sum which is decremented by one or two from actual sum. An incrementing stage of one or two will be introduced to modulo adder sum to get the actual sum. In scaling phase the overflow is avoided. In correction phase, it is guaranteed that no more than one addition operation is performed.

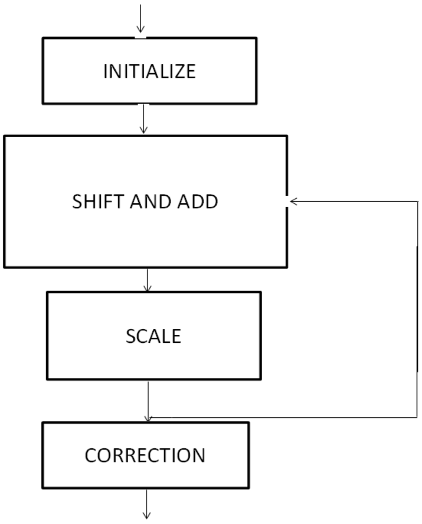
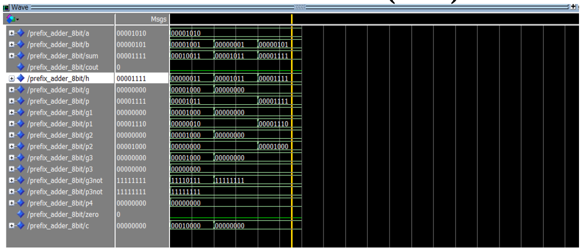


Fig 6: Proposed multiplier diagram

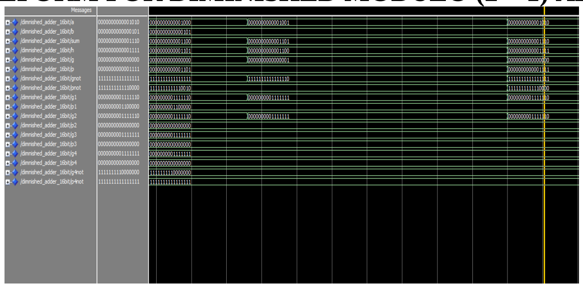
4. SIMULATION RESULTS:

WAVEFORM FOR MODULO (2^N+1) ADDER



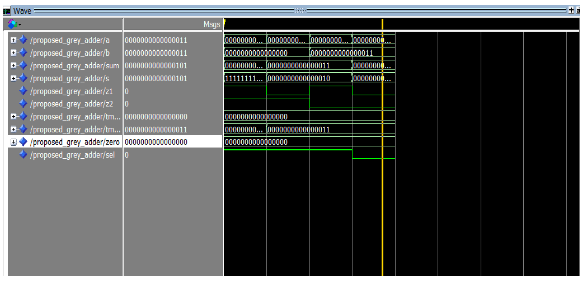
```
/prefix_adder_8bit/a      00001010
/prefix_adder_8bit/b      00000101
/prefix_adder_8bit/sum    00001111
/prefix_adder_8bit/cout   0
/prefix_adder_8bit/h      00001111
/prefix_adder_8bit/g      00000000
/prefix_adder_8bit/p      00001111
/prefix_adder_8bit/g1     00000000
/prefix_adder_8bit/p1     00001110
/prefix_adder_8bit/g2     00000000
/prefix_adder_8bit/p2     00001000
/prefix_adder_8bit/g3     00000000
/prefix_adder_8bit/p3     00000000
/prefix_adder_8bit/g3not  11111111
/prefix_adder_8bit/p3not  11111111
/prefix_adder_8bit/p4     00000000
/prefix_adder_8bit/zero   0
/prefix_adder_8bit/c      00000000
```

WAVEFORM FOR DIMINISHED MODULO (2^N+1) ADDER



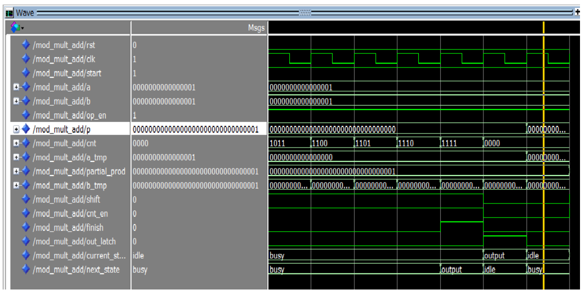
```
/dimnished_adder_16bit/a      0000000000001010
/dimnished_adder_16bit/b      0000000000000101
/dimnished_adder_16bit/sum    0000000000001110
/dimnished_adder_16bit/h      0000000000001111
/dimnished_adder_16bit/g      0000000000000000
/dimnished_adder_16bit/p      0000000000001111
/dimnished_adder_16bit/gnot   1111111111111111
/dimnished_adder_16bit/pnot   1111111111110000
/dimnished_adder_16bit/g1     0000000001111110
/dimnished_adder_16bit/p1     0000000001100000
/dimnished_adder_16bit/g2     0000000001111110
/dimnished_adder_16bit/p2     0000000000000000
/dimnished_adder_16bit/g3     0000000001111111
/dimnished_adder_16bit/p3     0000000000000000
/dimnished_adder_16bit/g4     0000000001111111
/dimnished_adder_16bit/p4     0000000000000000
/dimnished_adder_16bit/g4not  1111111110000000
/dimnished_adder_16bit/p4not  1111111111111111
```

WAVEFORM FOR PROPOSED DIMINISHED MODULO (2^N+1) ADDER



```
/proposed_grey_adder/a      0000000000000011
/proposed_grey_adder/b      0000000000000011
/proposed_grey_adder/sum    0000000000000101
/proposed_grey_adder/s      0000000000000101
/proposed_grey_adder/z1     0
/proposed_grey_adder/z2     0
/proposed_grey_adder/tm...  0000000000000000
/proposed_grey_adder/tm...  0000000000000011
/proposed_grey_adder/zero   0000000000000000
/proposed_grey_adder/sel    0
```

WAVEFORM FOR PROPOSED MULTIPLIER



/mod_mult_add/rst	0
/mod_mult_add/clk	1
/mod_mult_add/start	1
/mod_mult_add/a	0000000000000001
/mod_mult_add/b	0000000000000001
/mod_mult_add/op_en	1
/mod_mult_add/p	00000000000000000000000000000001
/mod_mult_add/cnt	0000
/mod_mult_add/a_tmp	0000000000000001
/mod_mult_add/partial_prod	00000000000000000000000000000001
/mod_mult_add/b_tmp	00000000000000000000000000000001
/mod_mult_add/shift	0
/mod_mult_add/cnt_en	0
/mod_mult_add/finish	0
/mod_mult_add/out_latch	0
/mod_mult_add/current_st...	idle
/mod_mult_add/next_state	busy

5. CONCLUSION

The drawback for the modulo adder is that it is not used for adding zero operands. The proposed adder will eliminate this drawback, and zero operands can be added effectively and fast.

A multiplier is developed from this proposed adder that can give fast and accurate output

REFERENCES:

[1] Haridimos T. Vergos, Member, IEEE, and Giorgos Dimitrakopoulos, Member, IEEE ":On Modulo 2n+1 Adder Design" IEEE TRANSACTIONS ON COMPUTERS, VOL. 61, NO. 2, FEBRUARY 2012

[2].Costas Efstathiou, Haridimos T. Vergos, Member, IEEE, and DimitrisNikolos, Member, IEEE "Modulo 2n _ 1 Adder Design Using Select-Prefix Blocks" IEEE TRANSACTIONS ON COMPUTERS, VOL. 52, NO. 11, NOVEMBER 2003.

[3].Dr. A. J. Al-Khalili's "Parallel prefix adders" under Concordia University.

[4]*G.Dimitrakopoulos, D. G. Nikolos, H. T. Vergos, D. Nikolos C. Efstathiou* "NEW ARCHITECTURES FOR MODULO 2*N* -1 ADDERS*"*.

[5].Haridimos T. Vergos, Costas Efstathiou, and DimitrisNikolos, Member, IEEE "Diminished One Modulo 2n+ 1 Adder Design" IEEE TRANSACTIONS ON COMPUTERS, VOL. 51, NO. 12, DECEMBER 2002.

[6].Haridimos T. Vergos, Member, IEEE, and Giorgos Dimitrakopoulos, Member, IEEE "On Modulo 2n +1 Adder Design" IEEE TRANSACTIONS ON COMPUTERS, VOL. 61, NO. 2, FEBRUARY 2012 173

[7].J. Al-Khalili COEN 6501 "Parallel Adders".

[8].Modulo 2n+1 Adder Using Circular Carry Selection" Proceedings of the World Congress on Engineering 2011 Vol II WCE 2011, July 6 - 8, 2011, London, U.K.

[9].Riyaz A. Patel, Mohammed Benaissa, Senior Member, IEEE, and Said Boussakta, Senior Member, IEEE "Fast Parallel-Prefix Architectures for Modulo 2n -1 Addition with a Single Representation of Zero" IEEE TRANSACTIONS ON COMPUTERS, VOL. 56, NO. 11, NOVEMBER 2007

[10].Ruchi Singh, R. A. Mishra "Design and Simulation of Diminished-One.

[11].Somayeh Timarchi, Keivan Navi "Improved Modulo 2*n* +1 Adder Design"

AUTHORS

Denny Oinam received the B.Tech. and studying M.E. degrees in Electronic and Communication Engineering from Pondicherry University and Anna University in 2008 and 2013, respectively.

K. Saravanan is now Assistant Professor in Veltech Multitech Dr.Rangarajan Dr.Sakunthal Engg.College,Chenna i, Tamil Nadu, India

Raja .M, Assistant Professor, Veltech Multitech Dr.Rangarajan Dr.Sakunthala Engg.College,Chennai, Tamil Nadu, India,

Yogaraj . A, Assistant Professor,Veltech Technical University Chennai, Tamil Nadu ,India,