Design and Simulation of Diminished-One Modulo 2^n+1 Adder Using Circular Carry Selection

Ruchi Singh, R. A. Mishra

***Abstract*— Diminished-one modulo 2^n+1 Adder using Circular carry selection (CCS) is an important building block of RNS based DSP system. In this paper, we have presented a Diminished-one modulo 2^n+1 adder using CCS scheme. The architecture design of Diminished-one modulo 2^n+1 adder using CCS consists of a Dual Sum-Carry Look Ahead Adder (DS-CLA), a Circular Carry Generator (CCG) and a Multiplexer (MUX). The adder has been simulated using verilog HDL codes and mapped this design to the TSMC (180nm) implementation technology using the Synopsys Design Complier and calculated the area, power Dissipation and Time delay for n = 8, 12, 16, 24, 32, 48, 64. We have compared our results with Select-Prefix method for n = 8, 16, 32 and 64 and found that the area occupied is lesser than Select-Prefix Method.**

***Index Terms*— VLSI Design, Residue number system (RNS), Modulo 2^n+1 adder, Diminished-one, Circular carry selection (CCS)**

I. Introduction

RESIDUE number system(RNS) is a non-weighted number system and it works well in the area where key operation required are addition, subtraction and multiplication such as digital filter, FFT, Image processing and digital communication [1], [2]. In RNS, addition, subtraction and multiplication are inherently carry free, i.e. each digits of the result is a function of only one digit of each operand, hence independent of all the other digits so complexity is reduced and operation can be executed in less time[1], [2]. In a standard Residue number system, RNS is defined by a set of pair-wise relative prime integer, $\{p_1, p_2, \ldots, p_n\}$ called moduli. A number R can be converted into residue representation $\{r_1, r_2, \ldots, r_n\}$, where $r_1, r_2, \ldots, r_n$ are the least positive remainders when dividing R by the $p_1, p_2, \ldots, p_n$. It is denoted by $r_i=|R|p_i$ for $i=1,\ldots.n$ [1], [2]. Residue arithmetic operation of two numbers A and B is defined by

$(C_1, C_2, \ldots\ldots, C_n) = (A_1, A_2, \ldots\ldots, A_n) \# (B_1, B_2, \ldots\ldots, B_n)$

Where # is either 'addition', 'subtraction' or 'multiplication' and A_i and B_i are residue representation of A and B.

There are many moduli sets like $(2^n-1, 2^n, 2^n+1)$[3], $(2^n-1, 2^n, 2^n+1, 2^{2n}+1)$[4], $(2^n-1, 2^n, 2^n+1, 2^{n+1}+1)$[5] etc. The most well-known three-moduli RNS that uses a base of the form $(2^n-1, 2^n, 2^n+1)$ has received significant attention, mainly due to the existence of very efficient combinational converters from/to the binary system. A 2^n+1 channel is also an integral part of the *5*-moduli RNS proposed in [6]. From the above it can be said that the design of efficient modulo 2^n+1 adder is vital in RNS-based applications.

Modulo 2^n+1 channel handles $n+1$ bit input where as modulo 2^n-1 and 2^n type can handle only n bit input operands. So, the implementation of modulo 2^n+1 channel is more complicated than 2^n-1 or 2^n type channel [7]. To remove this problem, we use Diminished-one arithmetic proposed by Leibowitz [8]. In Diminished-one arithmetic, the inputs A & B are represented by A^* and B^* where $A^* = A-1$ and $B^*= B-1$ so the concept of diminished-one makes $n+1$ bits to n bits wide.

Many papers have been presented on Diminished-one modulo 2^n+1 addition [7], [9]-[11].

Here, we have presented a paper on Diminished-One modulo 2^n+1 *a*dder Using CCS scheme which is based on paper [7]. This adder consists of a DS-CLA, a CCG and a MUX. The DS-CLA adder gives two modulo results in parallel and the CCG computes the carry out bit and circularly controls the MUX to find the correct modulo sum from DS-CLA adder.

The paper has been organized in four sections. In section II, the details of the Diminished-one modulo 2^n+1 Adder using CCS is presented. Section III gives the performance parameters comparison and the conclusion part is given in section IV.

II. Diminished-one modulo 2^n+1 Adder using Circular Carry Selection scheme

We have analyzed the Modulo adder using two methods, these methods are:

A. Direct equation Implementation Method

Let $A^* = a^*_{n-1}, \ldots., a^*_1, a^*_0$ and $B^* = b^*_{n-1}, \ldots., b^*_1, b^*_0$ are two numbers represented in Diminished-one format. The modulo 2^n+1 addition of A^* and B^* is given by $S^* = s^*_{n-1}, \ldots., s^*_1, s^*_0$ where

$$S^* = |\, A^* + B^* + \overline{c_{n-1}}\, | \tag{1}$$

Manuscript received February 16, 2011; revised April 05, 2011.
Ruchi Singh is P.G student of the Department of Electronics and Communication Engineering, Motilal Nehru National Institute of Technology, Allahabad, INDIA (e-mail: ruche.ec@ gmail.com).
R. A. Mishra is working as Assistant Professor in the Department of Electronics and Communication Engineering, Motilal Nehru National Institute of Technology, Allahabad, INDIA, (phone: 0532-2271467; fax: 0532-2445101; e-mail: ramishra@ mnnit.ac.in).

Here c_{n-1} is carry out bit of $(A^* + B^*)$ and given by equation as proposed by [7].

$$c_{n-1} = g^*_{n-1} + \sum_{j=0}^{n-2}\left(\prod_{k=j+1}^{n-1} p^*_k\right) g^*_j \qquad (2)$$

According to CLA function we take two terms.
Carry Generate term $g^*_i = a^*_i . b^*_i$
Carry Propagate term $p^*_i = a^*_i \oplus b^*_i$
Where $i = 0$ to $n-1$.
The diminished-one operators are

$$S^* = S - 1$$
$$g^*_i = g_i - 1$$
$$p^*_i = p_i - 1$$

The block diagram of CCS Diminished-one modulo 2^n+1 adder is shown in figure (1). The input to this block is A^* and B^* of n bit each. These inputs are applied to DS-CLA adder circuit. The DS-CLA adder produces two generate (g^*) and propagate (p^*) terms and gives three outputs, one is applied to CCG which is used to produce the carry-out bit c_{n-1}, and the other two outputs are $S^*_{i,1}$, $S^*_{i,0}$. The carry-out bit c_{n-1} is connected to an inverter and applied as a control signal to the MUX. If the $\overline{c_{n-1}}$ is '0' the output of MUX is $S^*_{i,0}$ otherwise the output is $S^*_{i,1}$. The output of MUX is connected to XOR gate. The other input to XOR gate is propagate term p^*_i and finally we get $S^*_i = s^*_{n-1}, \ldots, s^*_1, s^*_0$ which is given by the following equation as proposed by [9]:

$$S^*_i = \begin{cases} S^*_{i,1} = \left[g^*_{i-1} + \left\{ \sum_{j=0}^{i-2}\left(\prod_{k=j+1}^{i-1} p^*_k\right) g^*_i + \prod_{k=0}^{i-1} p^*_k \right\}\right] \oplus p^*_i & if\ c_{n-1} = 0 \\ S^*_{i,0} = \left[g^*_{i-1} + \sum_{j=0}^{i-2}\left(\prod_{k=j+1}^{i-1} p^*_k\right) g^*_i \right] \oplus p^*_i & if\ c_{n-1} = 1 \end{cases} \qquad (3)$$

For $n = 4$, the equations are

$$S^*_{3,1} = \{g^*_2 + (p^*_2 . p^*_1 . g^*_0) + (p^*_2 . g^*_1) + (p^*_2 . p^*_1 . p^*_0)\} \oplus p^*_3$$
$$S^*_{2,1} = \{g^*_1 + (p^*_1 . g^*_0) + (p^*_1 . p^*_0)\} \oplus p^*_2$$
$$S^*_{1,1} = \{g^*_0 + p^*_0\} \oplus p^*_1$$
$$S^*_{0,1} = \overline{p^*_0}$$
$$S^*_{3,0} = \{g^*_2 + (p^*_2 . p^*_1 . g^*_0) + (p^*_2 . g^*_1)\} \oplus p^*_3$$
$$S^*_{2,0} = \{g^*_1 + (p^*_1 . g^*_0)\} \oplus p^*_2$$
$$S^*_{1,0} = \{ g^*_0 \} \oplus p^*_1$$
$$S^*_{0,0} = p^*_0$$

The equations for $S^*_{i,0}$ and $S^*_{i,1}$ are same except the AND operation of propagate terms p^*_i in $S^*_{i,1}$ and $S^*_{0,1}$ is the compliment of $S^*_{0,0}$.

The complete circuit of CCS Diminished-one modulo 2^n+1 adder for $n=4$ is shown in fig. (2) as proposed by Tso-Bing Juang, Ming-Yu Tsai and Chin-Chieh Chiu [9].

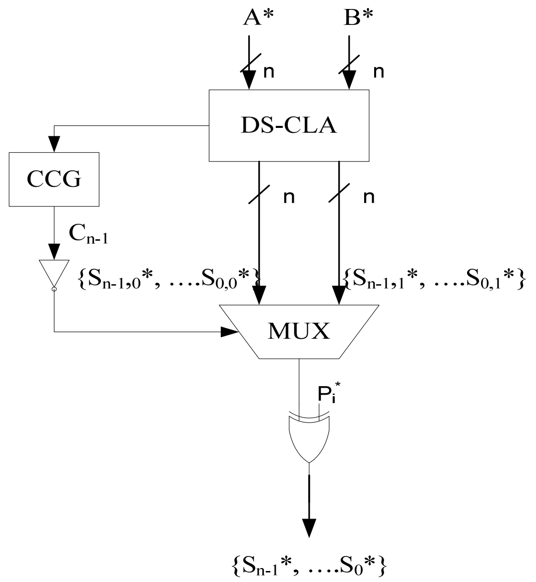

Fig.(1) Block diagram of CCS Diminished-one modulo 2^n+1 adder

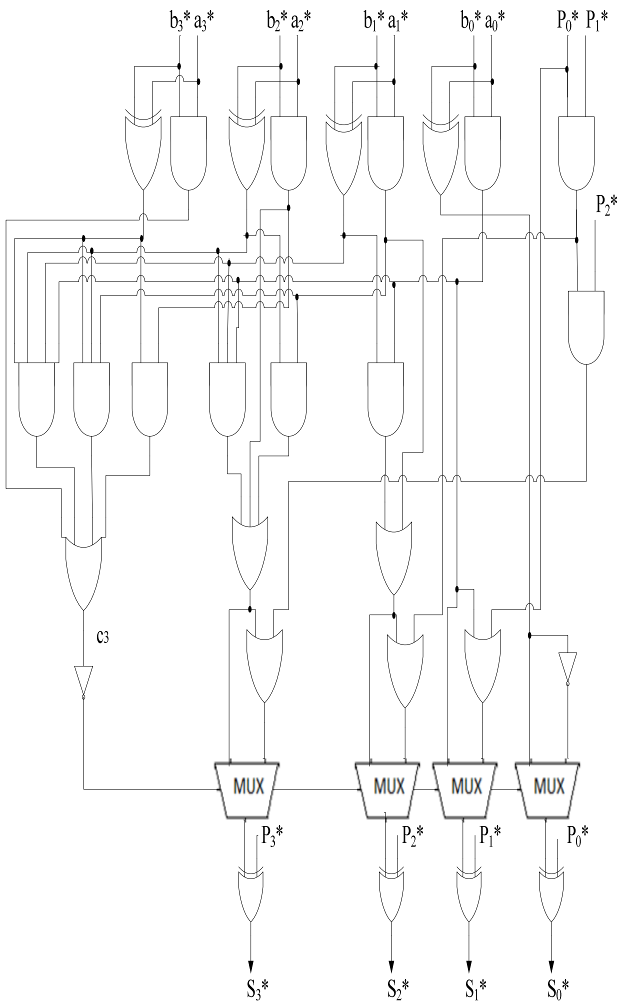

Fig.(2) logic diagram for CCS Diminished- one modulo 2^4+1 adder

B. *Partitioning circuit for large dimension*

For the large dimension of n, we partition the n bit CCS modular adder into m, r bits, which are given in paper [7]. Here $n = m \times r$

Where m = no. of DS-CLA blocks

ISBN: 978-988-19251-4-5
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

r = no. of inputs in a block

Both input data are divided into m block inputs

$A^* = a^*_{m-1}, \ \ldots, a^*_0$

$B^* = b^*_{m-1}, \ \ldots, b^*_0$

And Sum

$S_t^* = s^*_{(t+1)r-1}, \ldots, s^*_{tr+1}\, s^*_{tr}$

$\quad = A_t^* + B_t^* + k^*_{t-1}$

Where

k^*_{t-1} is carry-out bit

$A_t^* = a^*_{(t+1)r-1}, \ldots, a^*_{tr+1}\, a^*_{tr}$

$B_t^* = b^*_{(t+1)r-1}, \ldots, b^*_{tr+1}\, b^*_{tr}$

for $t = 0, \ldots\ldots, m\text{-}1$

Where k^*_{t-1} represents the carry-out bit of the $(t\text{-}1)^{th}$ addition block. In each r-bit CCS addition block, the DS-CLA Adder generates two block sums $S^*_{t,0} = S^*_t$ for $k^*_{t-1} = 0$ and for $k^*_{t-1} = 1$, $S^*_{t,1} = S^*_t$. So we can say that the carry-out bit k^*_{t-1} is used to select the correct block sum. Each carry-out bit k^*_{t-1} generated by CCG can be understood by these equations proposed by [7] as follows:

$$k^*_{t-1} = \left[G^*_{t-1} + \left\{\sum_{j=0}^{t-2}\left(\prod_{l=j+1}^{t-1} p_l^*\right)G_j^* + \overline{c_{n-1}}\prod_{l=0}^{t-1} p_l^*\right\}\right] \tag{4}$$

$$k^*_{t-1} = \begin{cases} k^*_{t-1,1} = \left[G^*_{t-1} + \left\{\begin{matrix}\sum_{j=0}^{t-2}\left(\prod_{l=j+1}^{t-1} p_l^*\right)G_j^* + \\ \prod_{l=0}^{t-1} p_l^*\end{matrix}\right\}\right] & if\ \ c_{n-1} = 0 \\ k^*_{t-1,0} = \left[G^*_{t-1} + \sum_{j=0}^{t-2}\left(\prod_{l=j+1}^{t-1} p_l^*\right)G_j^*\right] & if\ c_{n-1} = 1 \end{cases} \tag{5}$$

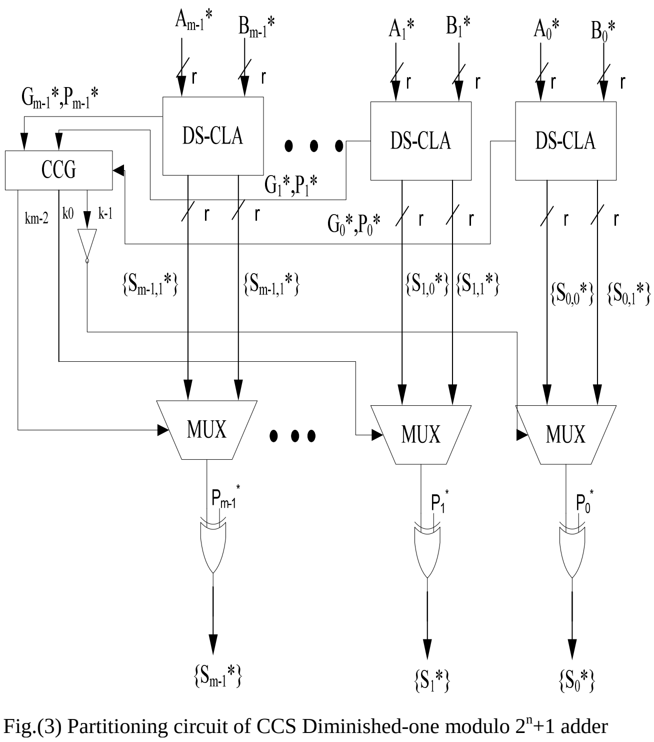

Fig.(3) Partitioning circuit of CCS Diminished-one modulo 2^n+1 adder

In (4), the block generate term

$$G_t^* = g^*_{tr+(r-1)} + \sum_{j=tr}^{tr+(r-2)}\left(\prod_{k=j+1}^{tr+(r-1)} p_k^*\right)g_j^* \tag{6}$$

And the block propagate term

$$P_t^* = \prod_{k=tr}^{tr+(r-1)} p_k^* \tag{7}$$

These two terms G_t^* and $P_t^*$are provided by the t^{th} CCS addition block. The carry-out bit c_{n-1} is used as k_{-1} in the CCS addition block as proposed by [7]. The equation for c_{n-1} is same as equation (2).

The block diagram of partitioning circuit of CCS Diminished-one modulo 2^n+1 adder is shown in figure (3). The input to this block is A^* and B^* of n-bit each. These inputs are applied to m no. of DS-CLA adder blocks according to r-bit inputs. Each DS-CLA adder blocks produces generate (G^*) and propagate (P^*) terms and it is applied to CCG block which is used to produce the carry-out bits k_t^*, and the other two outputs are $S^*_{m,1}$, $S^*_{m,0}$. The carry out bit k^*_{-t}, is connected to an inverter and then applied as a control signal to the MUX and the rest of carry-out bits are directly applied to the MUX as a control signal. If the $\overline{k^*_{-1}}$ is '0' the output of MUX is $S^*_{i,0}$ otherwise the output is $S^*_{i,1}$. The output of MUX is connected to XOR gate. The other input to the XOR gate is propagate term p_i^* and finally we get $S_i^* = s^*_{n-1}, \ldots, s^*_1, s^*_0$ which is given in equation (3) as proposed in [9].

III. Performance Parameters Evaluation

The CCS Diminished-one modulo 2^n+1 adder has been simulated using Verilog codes and mapped this design to the TSMC 180nm implementation technology using the Synopsys Design Complier for n = 8, 12, 16, 24, 32, 48, 64. For this, we have written Verilog HDL programs for Direct equation implementation method and for Partitioning circuit. Then calculated area, power dissipation and time delay using the Synopsys design compiler tool and shows the AT (Area × Delay) and TP (Delay × Power) products. All the area results are expressed in μm^2, delay results are based on the assumption of worst case commercial model which is given in *ns* and power dissipation results are expressed in mW.

The performance parameters and the AT and TP products in tabular form are shown in Table (1). The Direct equation methods are expressed as CCS and Partitioning methods are expressed as CCS $m \times n$.

In the paper, proposed by S.-H. Lin and M.-H. Sheu[7] they use the UMC 180nm technology on the Cadence PKS and Silicon Ensemble tool. They have used only Partitioning method for the same value of n. However, there are some corrections in paper [7] which is proposed in paper [9]. For comparison of the results there is no data in paper [9], so we have compared our results with the work proposed by C. Efstathiou, H. T. Vergos and and D. Nikolos [10]. They have verified their result using Hardware Description language and mapped this design to the VST Diplomat technology 250nm implementation technology using the Synopsys Design Complier. Table (2) shows the comparison of area and time delay of CCS Diminished-one modulo 2^n+1 adder using Equation method, Partitioning method and Select-Prefix method as proposed in paper [10] for n = 8, 16, 32 and 64. Area of CCS Diminished-one modulo adder using CCS is lesser than Select-Prefix method.

ISBN: 978-988-19251-4-5
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

TABLE I
PERFORMANCE PARAMETERS OF PROPOSED DIMINISHED-ONE MODULO 2^n+1 ADDER USING CCS

N	Architecture	Area(μm^2)	Power(mW)	Delay(ns)	AT	TP
8	CCS 2×4	1124.32	1.87	2.29	2574.69	4.28
	CCS	771.73	1.38	2.46	1898.46	3.40
12	CCS 3×4	1792.93	2.99	2.53	4536.11	7.57
	CCS	1437	2.36	2.66	3822.42	6.28
16	CCS 4×4	2408.31	4.01	2.54	6117.11	10.19
	CCS	2142.2	3.52	3.05	6533.71	10.74
24	CCS 2×12	4031.6	6.58	2.63	10603.11	17.31
	CCS 6×4	3702.28	6.54	2.97	10995.77	19.42
	CCS	3688.98	5.95	3.95	14571.47	23.50
32	CCS 2×16	5102.70	8.98	3.74	19084.1	33.59
	CCS 8×4	3702.28	9.01	2.96	10958.75	26.67
	CCS	5305.61	8.51	4.24	22495.79	36.08
48	CCS 4×12	7324.73	12.91	4.53	33181.03	58.48
	CCS 12×4	8259.45	13.46	2.97	24530.57	39.98
	CCS	9244.07	14.24	4.89	45203.5	69.63
64	CCS 4×16	10185.44	17.99	3.37	34324.93	60.63
	CCS 16×4	12088.14	19.21	3.05	36868.83	58.59
	CCS	14812.46	21.5	5.86	86801.02	125.99

TABLE II
PERFORMANCE PARAMETERS OF PROPOSED DIMINISHED-ONE MODULO 2^n+1 ADDER USING CCS

N	Architecture	Area(μm^2)	Delay(ns)
8	CCS 2×4	1124.32	2.29
	CCS	771.73	2.46
	Select-Prefix 2×4 [10]	3485.1	1.66
16	CCS 4×4	2408.31	2.54
	CCS	2142.2	3.05
	Select-Prefix 2×8 [10]	8338.7	1.80
	Select-Prefix 4×4 [10]	7752.5	1.85
32	CCS 2×16	5102.70	3.74
	CCS 8×4	3702.28	2.96
	CCS	5305.61	4.24
	Select-Prefix 2×16 [10]	14769.4	2.15
	Select-Prefix 4×8 [10]	15524.8	2.26
64	CCS 4×16	10185.44	3.37
	CCS 16×4	12088.14	3.05
	CCS	14812.46	5.86
	Select-Prefix 2×32 [10]	27544.6	2.78
	Select-Prefix 4×16 [10]	26999.7	2.67

IV. CONCLUSION

In this paper, we have implemented the CCS Diminished-one modulo 2^n+1 adder using two methods: first using Direct equation method and the second using Partitioning method. From the result shown in Table (1), it is clear that for n = 8 and 12, Equation method gives a lesser AT and TP product and for larger value of n , Partitioning method gives a better result. The shaded portion shows the best result for the same value of n. From Table (2) it is clear that area of Diminished-one modulo adder using Equation method and Partitioning method is lesser than Select-Prefix method for n = 8, 16, 32 and 64. By increasing value of n, area, power dissipation and time delay are increasing.

REFERENCES

[1] N. Szabo and R. Tanaka, Residue Arithmetic and its Applications to Computer Technology, McGraw-Hill, New York (1967).

[2] M.A. Soderstrand *et al.*, Residue Number System Arithmetic: Modern Applications in Digital Signal Processing, IEEE Press, New York (1986).

[3] Y.Wang,X.Song, M.Aboulhamid & H.Shen,“Adder-based residue to binary number converters for (2^n -1,2^n,2^n +1),”*IEEE Trans. Signal Process.*,vol.50,no.7,pp.1772–1779,Jul.2002.

[4] B. Cao, C. H. Chang, and T. Srikanthan, “An efficient reverse converter for the 4-moduli set based on the newchinese remainder theorem,” *IEEE Trans. Circuits Syst. I, Fundam. Theory Appl.*, vol. 50, no. 10, pp. 1296–1303, Oct. 2003.

[5] P. V. Ananda Mohan and A. B. Premkumar, “RNS-to-binary converters for two four-moduli sets” *IEEE Trans. Circuits Syst. I, Reg. Papers*, vol. 54, no. 6, pp. 1245–1254, Jun. 2007.

[6] Cao, C.H. Chang and T. Srikanthan, A residue-to-binary converter for a new 5-moduli set, *IEEE Trans. Circuits Syst. I* 54 (5) (2007), pp. 1041–1049.

[7] S.-H. Lin and M.-H. Sheu, “VLSI design of diminished-one modulo 2^n + 1 adder using circular carry selection,” *IEEE Trans. Circuits Syst. II, Exp. Briefs,* vol. 55, no. 9, pp. 897–901, Sep. 2008.

[8] L.M.Leibowitz,“A simplified binary arithmetic for the fermat number transform,” *IEEE Trans. Acous., Speech, Signal Process.*, vol. 24, pp. 356–359, 1976.

[9] Tso-Bing Juang, Ming-Yu Tsai, Chin-Chieh Chiu, “Correction to VLSI design of diminished-one modulo 2^n + 1 adder using circular carry selection,” *IEEE Trans. Circuits Syst. II, Exp. Briefs*, vol. 56, no. 3, pp. 260–261, Mar. 2009.

[10] C. Efstathiou, H. T. Vergos, and D. Nikolos, “Modulo 2^n±1 adder design using select-prefix blocks,” *IEEE Trans. Comput.,* vol. 52, no. 11, pp. 1399–1406, Jul. 2003.

[11] H.T.Vergos,C.Efstathiou,& D Nikolos,“Diminished-one modulo 2^n+1 adder design,” *IEEE Trans. Comput.,* vol. 51, no. 12, pp. 1389–1399, Dec. 2002.