# Design of Reverse Converter Using Parallel Prefix Adders and CRT

J.Brindha Devi, G. Rohinipriya

***Abstract*— The efficient design of Residue Number System (RNS) reverse converter based on Parallel Prefix Adder and Chinese Remainder Theorem is analyzed. In nowadays system, to achieve high speed reverse converter by the use of parallel prefix adder. And also the parallel prefix based adder components is used to solve the high power consumption problem and provide better tradeoff between power consumption and delay. The parallel prefix adder structure can implement by interconnecting only small number of different modules.**

***Index Terms*—Reverse converter, RNS, CRT.**

## I. INTRODUCTION

The residue number system (RNS) plays significant role due to its low power consumption features and reasonable delay. The Residue Number System can provide carry free and fully parallel arithmetic operations for several applications such as digital signal processing and also cryptography. the RNS is Non- weighted Number system capable of providing a parallel carry free arithmetic. It can map large number to small residues without any need for carry propagation. For successful RNS based application, the choice of moduli set and hardware design of residue to binary conversion is very important. The residue to binary conversion is time consuming and hard operation. The approach to improve the performance of converters is: (i) a novel arithmetic formulation and new algorithms are design to achieve simplified conversion formulas. (ii) New moduli sets are introduced, that can lead to more simple calculations. There are several well known adder architecture such as carry save adder and ripple carry architecture are used to implement carry propagate adder, in that fast and expensive adders are carry look ahead or parallel prefix adder. To design the fast reverse converter , parallel prefix architecture is employed. The usage of parallel prefix adder architecture ti to implement converters, it increases the speed and also increase the area and power consumption. This increase of power consumption makes the reverse converter is not competitive.

### A. Analogous Work

The main parts of the Residue Number System (RNS) are the forward converter, modulo arithmetic units and the reverse converter. The reverse converter consists of complex and non-modular architecture. The significant effects on the reverse converter performance based on the moduli set and conversion algorithm. So that different moduli set have been introduced and also the selection of hardware components is also important for the RNS performance. The parallel prefix adders with high speed feature have used in RNS modular arithmetic channels. The performance gain due to parallel carry computation structures, based on different algorithm such as Sklansky and Kogge-Stone have maximum and minimum fan out and provide minimal logic depth.

.

## II. PROSPECTIVE METHOD

### A. Parallel prefix based components

The Chinese remainder theorem (CRT) depends on the RNS reverse conversion, can be directly mapped to Ripple Carry Adders (RCA). This leads to speed degradation, due to linear increase of the delay in the Ripple Carry Adder with minimum number of bits. Parallel prefix adder used in RNS reverse converters to bind the delay to logarithmic growth. In reverse converters, many number of parallel prefix adders are required. If one adder is used, the bit length of the adder is large; this results in high power consumption. To achieve the final binary representation, one regular binary addition is required in reverse converter structures. This final addition has the total delay of the converter due to large bit length of the operands.

### B.Residue Number System

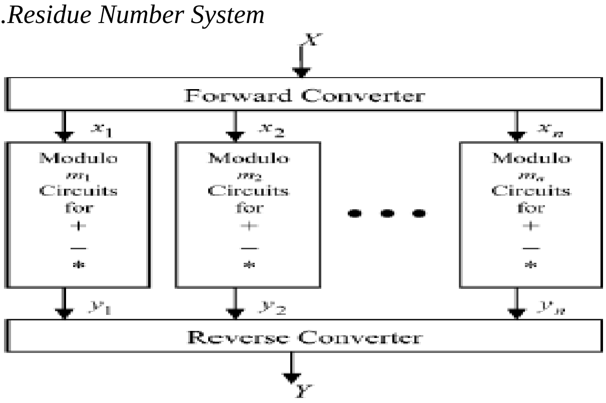

$X$
Forward Converter
$x_1$
$x_2$
$x_n$
Modulo $m_1$ Circuits for + — *
Modulo $m_2$ Circuits for + — *
Modulo $m_n$ Circuits for + — *
$y_1$
$y_2$
$y_n$
Reverse Converter
$Y$

Fig.1.RNS

The residue number system (RNS) is a non-weighted number system which speeds up arithmetic operations by dividing them into smaller parallel operations.

Since the arithmetic operations in each moduli are independent of the others, there is no carry propagation among them and so RNS leads to carry-free addition, multiplication and borrow-free subtraction. RNS is one of the most effective techniques for reducing the power dissipation in VLSI systems design. A Residue Number System (RNS) is an integer number representation system which, speeds up arithmetic computations by decomposing a number X into a set of elements, say ($x_1$,$x_2$,.... $x_n$), called the residues of the integer X with respect to a moduli set {$m_1$,$m_2$,…$m_n$}.

### C.Parallel prefix block

**J.Brindha Devi,** Assistant Professor, Department of ECE, Raja College of Engineering and Technology, Madurai, Tamilnadu,
**G. Rohinipriya** Assistant Professor, Department of ECE, Raja College of Engineering and Technology, Madurai, Tamilnadu

The parallel prefix structure consists of three main blocks, they are

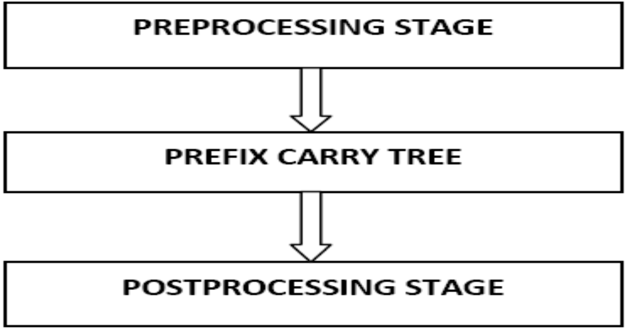


Fig.2. Parallel Prefix Structure

- Pre processing Stage
- Prefix carry tree
- Post processing stage

The parallel prefix adder operation begins with preprocessing stage by generating the Generate(Gi) and Propagate (Pi). The prefix carry tree get proceeded with the previous block signal to yield all carry bit signal and these stage contains three logic complex cells such as Black cell, Gray cell, and Buffer cell. Black cell compute both the propagate (P(i,j)) and generate (G(i,j)). The gray cell executes only the generate (G(i,j)). The carry bits generated in the second stage get passed to the post processing block thereby generating the sum.

: *Operation Of Parallel Prefiix Structure*

Gm:n=An AND Bn --- 1

G0 =Cin --- 2

Pm:n=An XOR Bn ---3

P0 = 0 --- 4

Gm:n=Gn:k OR Pn:k AND Gk-1:n ---5

Pm:n=Pn:k AND Pk-1:j ---6

Sn =Pn XOR Cin ---7

The Brent Kung adder prefix structure is to achieve the higher speed with reduced power consumption. On comparing with other parallel prefix adder, the BK adder is chosen for minimum fanout and should be higher speed in operation than others. The structure is elaborated for the proposed design having the modulo addition of (4n+1) for n=5.

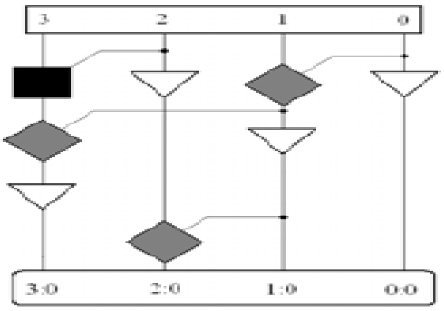


Fig. 3. 4 bit BK Adder Structure

*D. HMPE Structure (Hybrid Modular Parallel-Prefix Excess One Adder)*

The HMPE structure consists of two parts

i) Regular prefix adder

ii) Modified Excess One Unit

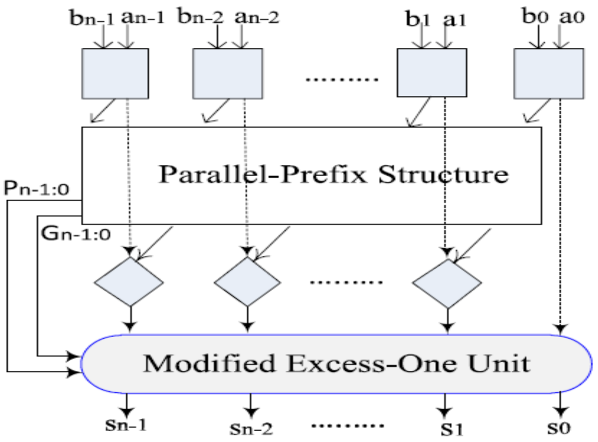


Fig.4. Hybrid Modular Parallel Prefix Excess One Adder

In HMPE structure, the two operands are added using the parallel prefix adder structure, and adder result is conditionally incremented based on control signals generated by the prefix section to assure the single zero representation.

The HMPE structure is highly flexible, it can be used with every prefix networks. Hence, the circuit performance parameters such as area, delay, and power-consumption can be adjusted by selecting the desired prefix structure.

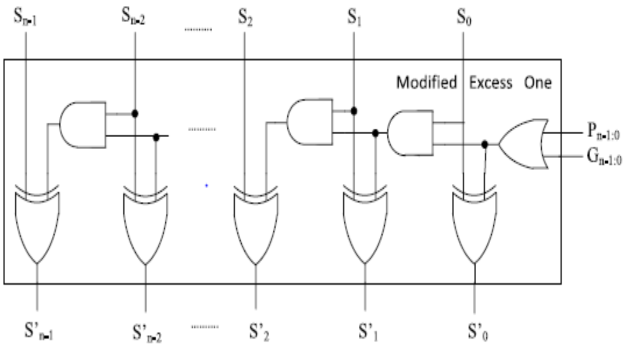


Fig. 5. Modified Excess one unit

To address this problem by eliminating the additional prefix level, instead of using a modified excess-one unit. The modified excess one unit is able to perform a conditional increment based on control signals. Kogge-Stone adder prefix structure is used in HMPE to achieve the high speed with reduced area cost. In the Modular parallel prefix excess one unit, Three logic-level basic cells are used for the kogge-stone adder based HMPE and Brent-kung adder based HRPX in the modified high speed reverse converter design.

*E. Reverse Converter*

The correct selection of a moduli set plays an important role in the design of the RNS systems because speed of RNS arithmetic unit as well as complexity of residue to binary converter depends on the form and the number of the moduli set. Another important one for reverse converter design is the selection of an proper conversion algorithm. The algorithms of reverse conversion are mainly based on Chinese remainder theorem (CRT), mixed-radix conversion (MRC) and new Chinese remainder theorems (New CRTs). From that, New CRTs have simple computations and can efficiently realize in hardware.

A weighted number can be X represented as X =$(x_1,x_2,\ldots, x_n)$,

Where

$$x_i = X \bmod P_i = |X|_{P_i}, 0 \le x_i < P_i \quad \text{-- (1)}$$

New Chinese Remainder Theorem 1: For the 4-moduli set { $p_1$ ,$p_2$ ,$p_3$ ,$p_4$} ,X the number can be converted from its residue representation by New CRT-I as follows:

$$X = x_1 + P_1 \left| \begin{matrix} k_1(x_2 - x_1) + k_2P_2(x_3 - x_2) \\ +k_3P_2P_3(x_4 - x_3) \end{matrix} \right|_{P_2P_3P_4} \quad \text{--- (2)}$$

Where

$$\begin{aligned} &|k_1 \times P_1|_{P_2P_3P_4} = 1 \\ &|k_2 \times P_1 \times P_2|_{P_3P_4} = 1 \\ &|k_3 \times P_1 \times P_2 \times P_3|_{P_4} = 1 \end{aligned} \quad \text{--- (3)}$$

New Chinese Remainder Theorem 2: by New CRT-II, with the 4-moduli set{$p_1$,$p_2$,$p_3$,$p_4$},the number X can be calculated from its corresponding residues ($x_1$,$x_2$,$x_3$,$x_4$) using the following equations.

Where

$$\begin{aligned} X &= Z + P_1P_2 \, |k_1(Y - Z)|_{P_3P_4} \\ Z &= x_1 + P_1 \, |k_2(x_2 - x_1)|_{P_2} \\ Y &= x_3 + P_3 \, |k_3(x_4 - x_3)|_{P_4} \end{aligned}$$

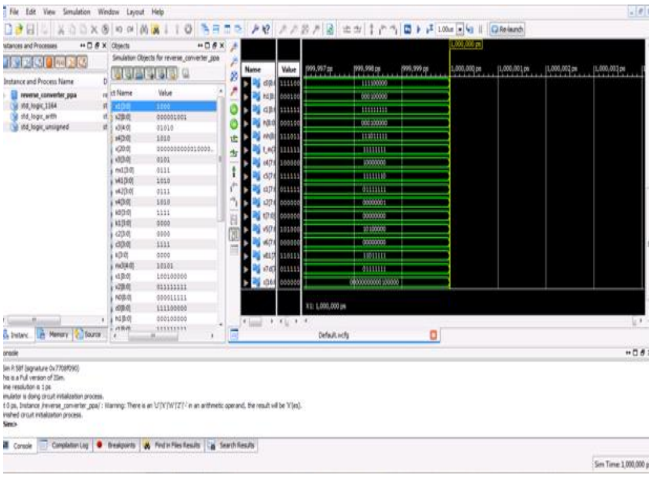
$$\begin{aligned} |k_1P_1P_2|_{P_3P_4} &= 1 \\ |k_2P_1|_{P_2} &= 1 \\ |k_3P_3|_{P_4} &= 1 \end{aligned} \quad \text{--- (4)}$$

New CRT II and I are applied to derive efficient reverse conversion algorithms for the new moduli sets {$2^n - 1$, $2^n$, $2^{2n}$, $2^{2n+1} - 1$} and {$2^n - 1$, $2^n + 1$, $2^{2n}$, $2^{2n} + 1$}, respectively.

## IV. RESULTS AND DISCUSSIONS

.

The simulation result of reverse converter design. where n=4, then the 4 residues are $x_1$,$x_2$,$x_3$ & $x_4$ and inputs are denoted as x1,x2,x3, and x4 . The weighted binary number is obtained from New CRT based algorithm for 4n-bit moduli set. Shown in Fig. Output will be obtained from residues and is denoted as 'X' in figure. ($2^{2n}$- 1) modulo addition in reverse converter is performed by HMPE adder component. (4n+1) addition of reverse converter is performed by HMPE & HRPX adder components.



```
ISim P.58f (signature 0x7708f090)
This is a Full version of ISim.
Time resolution is 1 ps
Simulator is doing circuit initialization process.
at 0 ps, Instance /reverse_converter_ppa/ : Warning: There is an 'U'|'X'|'W'|'Z'|'-' in an arithmetic operand, the result will be 'X'(es).
Finished circuit initialization process.
ISim>
```

Fig.6. Output for Reverse Converter

Table 1.Comparison table for existing and proposed system

| Parameters | Existing system (CSA) | Proposed system (HMPE & HPRX BK) |
|---|---|---|
| Delay | 5.760ns | 5.514ns |
| Area | Number of inputs in existing system is 145 | Number of inputs in proposed system is 81 |
| Power | 0.052W | 0.034W |

## V. CONCLUSION

The reverse converter for 4n-bit moduli set with n=4 has been designed, simulated and synthesized. The current reverse converter architectures is applied to enhance their performance and adjust the cost and performance parameters. A new parallel prefix based adder components were introduced to provide the required tradeoff between performance and cost. The components are specially designed for reverse converters. Implementation results shows that the reverse converters based on these components improve the speed. When compared with the original converters, the proposed converter, reduce the power consumption .

## REFERENCES

[1] S. Antao and L. Sousa, "The CRNS framework and its application to programmable and reconfigurable cryptography," ACM Trans. Archit. Code Optim., vol. 9, no. 4, p. 33, Jan. 2013.

[2] B. Cao, C. H. Chang, and T. Srikanthan, "An efficient reverse converter for the 4-moduli set {$2^n - 1$, $2^n$, $2^n + 1$, $2^{2n} + 1$} based on the new Chinese remainder theorem," IEEE Trans. CircuitsSyst. I, Fundam. Theory Appl., vol. 50, no. 10, pp. 1296–1303, Oct. 2003.

[3] J. Chen and J. Hu, "Energy-efficient digital signal processing via voltage over scaling-based residue number system," IEEE Trans. Very Large Scale Integr. (VLSI) Syst., vol. 21, no. 7, pp. 1322–1332, Jul. 2013.

[4] A. S. Molahosseini, K. Navi, C. Dadkhah, O. Kavehei, and S. Timarchi, "Efficient reverse converter designs for the new 4-moduli sets {$2^n - 1$, $2^n$, $2^n + 1$, $2^{2n+1} - 1$} and {2n − 1, 2n + 1, 22n, 22n + 1} based on new CRTs," IEEE Trans. Circuits Syst. I, Reg. Papers, vol. 57, no. 4, pp. 823–835, Apr. 2010.

[5] A.S. Molahosseini, S. Sorouri, and A. A. E. Zarandi, "Research challenges in next-generation residue number system architectures," in Proc. IEEE Int. Conf. Comput. Sci. Educ., Jul. 2012, pp. 1658–1661.

[6] K. Navi, A. S. Molahosseini, and M. Esmaeildoust, "How to teach residue number system to computer scientists and engineers," IEEE Trans. Educ., vol. 54, no. 1, pp. 156–163, Feb. 2011.

[7] B. Parhami, Computer Arithmetic: Algorithms and Hardware Designs, 2nd ed., New York, NY, USA: Oxford Univ. Press, 2010.

[8] C.H. Vun, A. B. Premkumar, and W. Zhang, "A new RNS based DA approach for inner product computation," IEEE Trans. Circuits Syst. I,Reg. Papers, vol. 60, no. 8, pp. 2139–2152, Aug. 2013.

[9] Y. Wang, X. Song, M. Aboulhamid, and H. Shen, "Adder based residue to binary numbers converters for ($2^n - 1$, $2^n$, $2^n + 1$)," IEEE Trans.N Signal Process., vol. 50, no. 7, pp. 1772–1779, Jul. 2002.