

International Journal of Advanced Research in Computer and Communication Engineering ISO 3297:2007 Certified Vol. 5, Issue 8, August 2016

# An Efficient Reverse Converter Design for Five Moduli Set RNS

Y. Ayyavaru Reddy<sup>1</sup>, B. Sekhar<sup>2</sup>

P.G.Scholar, Department of Electronics and Communication Engineering, Annamacharya Institute of Technology and

Sciences, Rajampet, Andhra Pradesh, India<sup>1</sup>

Assistant Professor, Department of Electronics and Communication Engineering, Annamacharya Institute of

Technology and Sciences, Rajampet, Andhra Pradesh, India<sup>2</sup>

Abstract: For designing high speed digital systems, it considered so many factors, among those the Number System, what it uses plays a crucial role. The Residue number system provides the inherent properties such as Carry-free operations, Parallelism and Fault Tolerance. While designing RNS, the selection of choice of moduli set plays a key role. The 3n-bit dynamic range RNS moduli set  $\{2^{n-1}, 2^n, 2^{n+1}\}$  is the most famous RNS moduli set because of its simple and well formed balanced moduli. However, the arithmetic operations with respect to the modulus 2<sup>n+1</sup> are complex and dynamic range is not sufficient for applications that require larger dynamic range. The 4n-bit dynamic range four moduli set minimize the dynamic range, asymmetric moduli channel length and long conversion delay. In this paper review on, a special five moduli set  $(2^{n}-1, 2^{n}, 2^{n}+1, 2^{n+1}-1, 2^{n-1}-1)$  for even n. It exploits the special properties of the numbers of the form  $2^{n}\pm 1$ , and extends the dynamic range of present triple moduli  $\{2^{n-1}, 2^{n}, 2^{n+1}\}$  based systems. It has dynamic range that can represent up to 5n-1 bits while keeping the moduli small enough and converter efficient. In this review paper reverse converter design is done with the Chinese Remainder Theorem (CRT) and the results are compared with the Mixed Radix Conversion theorem and also with three and four moduli sets.

Keywords: Residue Number System (RNS), Chinese Remainder Theorem (CRT), Dynamic Range (DR), Mixed Radix Conversion.

#### 1. INTRODUCTION

The Residue Number System is a very old number system.  $\{x_1, x_2, ..., x_n\}$  is a set of smaller integers used to represent It was founded by Sun Tzu. The basic idea of the RNS is integer X. When the integer X is divided by modulus m<sub>i</sub>, based on uniquely representing large binary numbers using the least positive remainder is obtained is called the a set of smaller residues, which results in carry-free, high-residue x<sub>i</sub>. It can be given as: speed and parallel arithmetic operations [1] [2]. This system is based on modulus operation, where the divider is called modulo and the remainder of the division operation is called residue. This fact encourages the implementation An alternative notation is given as of RNS in some applications where intensive processing is inevitable.

The main characteristic that distinguishes the RNS from other number systems is that the standard arithmetic operations; addition, subtraction and multiplication are easily implemented, whereas operations such as division, root, comparison, scaling and overflow and sign detection are much more difficult. Therefore, the RNS is very useful in applications that require a large number of addition and The RNS based system contains three major blocks, such multiplication, and a minimum number of comparisons, divisions and scaling. In other words, the RNS is preferable in applications in which additions and multiplications are critical. Such applications are cryptography, Digital Signal Processing, image processing, speech processing and transforms [1]-[3].

The RNS is an unconventional number system i.e., defined in terms of relatively Prime Moduli Set  $\{m_1, m_2, \dots, m_n\}$ that GCD  $(m_i, m_i) = 1$  for  $i \neq j$ . The residue set is given as

X mod  $m_i = x_i$ 

 $|X|_{mi} = x_i$ 

The Dynamic Range is the multiplication of the modulus of the moduli set  $\{m_1, m_2, ..., m_n\}$  and is denoted by M. Mathematical it is given as

$$M=m_1*m_2*....*m_n$$
 or  $M=\pi_{i=1}^n m_i$ 

as Forward Converter, RNS Processor and Reverse Converter. The Forward converter is used to convert weighted –binary number to Residue number. This process is simple and fast. RNS processer performs the required operations such as addition, subtraction and multiplication on the given residue numbers and it gives it to the reverse converter, it is also simple and fast. Reverse converter is used to convert Residue number to weighted-binary conversion [3]. The Reverse conversion process is more



## International Journal of Advanced Research in Computer and Communication Engineering

**ISO 3297:2007 Certified** Vol. 5, Issue 8, August 2016

difficult and introduces more overhead in terms of speed and complexity. For reverse conversion two algorithms are available namely Chinese remainder theorem (CRT) and mixed radix conversion (MRC). The CRT is desirable because the data conversion can be parallelized, while MRC is sequential process by its nature, it has less complex circuitry and slow modulo-M-operation, for different radixes. Whereas CRT requires large modulus adders operation in parallel manner. two more modulus to the triple moduli set, then the closed form multiplicative inverses become complex and cannot be implemented with simple hardware as in the case of triple moduli set. Four moduli superset  $\{2^{n-1}, 2^n, 2^{n+1}, 2^{n+1}\}$  is proposed, but here two of the moduli are in the form of  $2^n+1$ , which cause increase in dynamic range [7]. They also proposed a new supplementary four moduli superset  $\{2^{n-1}, 2^n, 2^{n+1}, 2^{n+1}-1\}$  with efficient conversion in its residue- to -binary converter which minimizes the

## 1.1 Chinese Remainder Theorem (CRT):

Consider the moduli set  $S = \{m_1, m_2, m_3, ..., m_n\}$  and let the and it has asymmetric moduli channel length and long RNS representation of an integer X conversion delay. A five moduli set  $\{2^{n-1}, 2^n, 2^{n+1}, be\{x_1, x_2, x_3, ..., x_n\}$ . Then the Chinese Remainder Theorem reconstructs X from its residues as follows two moduli are not in the form of  $2^n$  or  $2^n \pm 1$ . This makes

$$X = (X_1M_1Y_1 + X_2M_2Y_2 + ... + X_nM_nY_n) \mod M$$

Alternately, we can have

$$X=(\sum X_i M_i Y_{i}) \mod M$$
 where i=1 to n

Where,

 $\begin{array}{l} M \! = (m_1 ^* m_2 ^* m_3 ^* .... m_n) \\ M_i \! = M \! / m_i \ \ and \ \ Y_i \! = (M_i ^{-1}) \ mod \ m_i \end{array}$ 

#### 1.2 Mixed Radix Conversion (MRC):

Given an RNS number X be  $\{x_1, x_2, x_3, \dots, x_k\}$  for the moduli set  $\{m_1, m_2, m_3, \dots, m_k\}$ , the decimal equivalent of it can be computed as

 $X=a_1+a_2m_1+a_3m_1m_2+...+a_km_1m_2m_3...m_{k-1}$ 

Where the Mixed Radix Digits (MRD) can be computed as:

 $\begin{array}{l} a_1 = x_1 \\ a_2 = |(x_2 - a_1)|m_1^{-1}|m_2|m_2 \\ a_3 = |((x_3 - a_1)m_1^{-1}|m_3 - a_2)|m_2^{-1}|m_3|m_3 \\ \vdots \end{array}$ 

 $a_k = |(((x_k-a_1)|m_1^{-1}|m_k-a_2)|m_2^{-1}|m_k-...-a_{k-1})|m_{k-1}^{-1}|m_k|m_k$ For the MRDs  $a_i, 0 \le a_i \le m_i$ , any positive number in the interval  $\{0, \pi_{i-1}^{-k}m_{i-1}\}$  can be uniquely represented.

### 2. SELECTION OF MODULI SET

In RNS, the most important issues that must be taking into account are, a proper moduli set selection, forward conversion, residue arithmetic units (RAU), and reverse conversion. Majority of the high performance reverse converter architectures available are based on the three moduli set  $\{2^{n-1}, 2^n, 2^{n+1}\}$  [3]-[6]. However, this popular set is inefficient if increased parallelism is required to benefit from the residue arithmetic. It is inefficient in dealing with Subst a large dynamic range. One way to overcome this X = y inadequacy is to add extra moduli to this set from the same X=2+1 family  $(2^n \pm 1)$ . But it can be shown that if we add one or X=11

be implemented with simple hardware as in the case of  $2^{n+1}+1$  is proposed, but here two of the moduli are in the form of  $2^{n}+1$ , which cause increase in dynamic range [7]. They also proposed a new supplementary four moduli superset  $\{2^{n-1}, 2^n, 2^{n+1}, 2^{n+1}-1\}$  with efficient conversion in its residue- to -binary converter which minimizes the dynamic ranges [8]. Another class of conjugate moduli set is proposed [6]. But the moduli in these works are not pair wise relatively prime, hence it minimizes dynamic range, and it has asymmetric moduli channel length and long two moduli are not in the form of  $2^n$  or  $2^n \pm 1$ . This makes it hard to design efficient VLSI architectures. Another new five moduli set is  $\{2^{n+1}, 2^{n}-1, 2^{n}+1, 2^{n+1}-1, 2^{n+1}+1\}$ , where all the moduli are in the form of  $2^n$  or  $2^n \pm 1$ . Therefore, it has more efficient RAU. But the disadvantage is that the moduli set is not co-prime for any value of n, which reduces the dynamic range and also makes the residue-tobinary conversion algorithm complex. In this paper, we propose a new five moduli superset  $(2^{n}-1, 2^{n}, 2^{n}+1, 2^{n+1}-1)$ ,  $2^{n-1}$ -1) for even values of n. The forward and reverse converter and the modular operations for this moduli set is more efficient, as the moduli are in the form of  $2^n$  or  $2^n \pm 1$ . There is only one modulus in the form of  $2^{n}+1$ .

#### 3. REVERSE CONVERTER DESIGN FOR FIVE MODULI SET USING MRC

In the existing method the reverse converter was designed for three, four and five moduli set using mixed radix conversion theorem. The MRC is a sequential process so it has high conversion delay and slow modulo additions.

## 3.1: THEORETICAL CALCULATIONS: 3.1.1: 3 MODULI SET

Moduli set m= {m<sub>1</sub>, m<sub>2</sub>, m<sub>3</sub>} = {3, 4, 5} and Residue set x={x<sub>1</sub>, x<sub>2</sub>, x<sub>3</sub>} = {2, 3, 1}

The MRC can be given as  $X=y_1+y_2m_1+y_3m_2m_1 \rightarrow (1)$ 

Where 
$$y_1 = x_1 = 2$$
  
 $y_2 = ||m_1|^{-1}m_2 (x_2 - y_1)||_{m2}$   
 $|m_1|^{-1}m_2 = |3|^{-1} 4$   
 $3*k_1 = (1 \mod 4)$   
 $k_1 = 3$   
 $y_2 = |3*(3-2)|4 = |3|4 = 3$   
 $y_3 = |(m_2m_1)^{-1}m_3 (x_3 - (y_2m_1 + y_1))||_{m3}$   
 $(m_2m_1)^{-1}m_3 = (4*3)^{-1} 5 = |12|^{-1} 5$   
 $12*k_2 = (1 \mod 5)$   
 $k_2 = 3$   
 $y_3 = |3 \{1 - (3*3 + 2)\}|_5 = |-30|_5 = 0$   
Substitute all values in equation (1)  
 $X = y_1 + y_2m_1 + y_3m_2m_1$   
 $X = 2 + 3*3 + 0*12$   
 $Y_{-11}$ 



International Journal of Advanced Research in Computer and Communication Engineering ISO 3297:2007 Certified

Vol. 5, Issue 8, August 2016

## 3.1.2: 4 MODULI SET

set  $x = \{x_1, x_2, x_3, x_4\} = \{1, 2, 3, 4\}$ The MRC can be given as  $+y_4m_3m_2m_1$  $\rightarrow$  (1) Where  $y_1 = x_1 = 1$  $y_2 = ||m_1|^{-1}m_2(x_2-y_1)||_{m_2}$  $|\mathbf{m}_1|^{-1}_{\mathbf{m}2} = |5|^{-1}_{7}$  $5 K_1 = (1 \mod 7)$  $K_1=3$  $y_2 = |3^*(2-1)|_7 = |3|_7 = 3$  $y_3 = |(m_2m_1)^{-1}m_3(x_3-(y_2m_1+y_1))|_{m_3}$  $(m_2m_1)^{-1}_{m_3} = (7*5)^{-1}_8 = |35|^{-1}_8$  $35 K_2 = (1 \mod 8)$  $3 K_2 = (1 \mod 8)$  $K_2 = 3$  $y_3 = |3 \{3-(3*5+1)\}|_8 = |-39|_8 = 1$  $y_4 = |(m_3m_2m_1)^{-1}{}_{m4}(x_4 - (y_3m_2m_1 + y_2m_1 + y_1))|_{m4}$  $(m_3m_2m_1)^{-1}_{m4} = (8*7*5)^{-1}_{9} = |280|^{-1}_{9}$  $280 K_3 = (1 \mod 9)$  $1 K_3 = (1 \mod 9)$  $K_3=1$  $y_4 = |1* \{4 - (1*7*5+3*5+1)\}|_9 = |-47|_9 = 7$ Substitute all values in equation (1)  $X = y_1 + y_2 m_1 + y_3 m_2 m_1 + y_4 m_3 m_2 m_1$ X = 1 + 3 + 5 + 1 + 7 + 5 + 7 + 8 + 7 + 5X=2011

## 3.1.3: 5 MODULI SET

Moduli set m=  $\{m_1, m_2, m_3, m_4, m_5\} = \{15, 16, 17, 31, 7\}$ Residue set  $x = \{x_1, x_2, x_3, x_4, x_5\} = \{7, 13, 4, 2, 3\}$ The MRC can be given as  $X = y_1 + y_2 m_1 + y_3 m_2 m_{1+} y_4 m_3 m_2 m_1 + y_5 m_4 m_3 m_1$ Where  $y_1 = x_1 = 7$  $y_2 = ||m_1|^{-1}m_2(x_2-y_1)||_{m_2}$  $|\mathbf{m}_1|^{-1}_{\mathbf{m}2} = |\mathbf{15}|^{-1}_{\mathbf{16}}$  $15 K_1 = (1 \mod 16)$  $K_1 = 15$  $y_2 = |15^*(13-7)|_{16} = |90|_{16} = 10$  $y_3 = |(m_2m_1)^{-1}m_3(x_3-(y_2m_1+y_1))|m_3$  $(m_2m_1)^{-1}_{m3} = (16*15)^{-1}_{17} = |240|^{-1}_{17}$  $240 K_2 = (1 \mod 17)$  $2 K_2 = (1 \mod 17)$  $K_2 = 9$  $y_3 = |9^* \{4 - (10^*15 + 7)\}|_{17} = |-1377|_{17} = 0$  $y_4 = |(m_3m_2m_1)^{-1}_{m4} (x_4 - (y_3m_2m_1 + y_2m_1 + y_1))|_{m4}$  $(m_3m_2m_1)^{-1}_{m4} = (17*16*15)^{-1}_{31} = |4080|^{-1}_{31}$  $4080 K_3 = (1 \mod 31)$  $19 K_3 = (1 \mod 31)$  $K_3 = 18$  $y_4 = |18* \{2-(0+150+7)\}|_{31} = |-2790|_{31} = 0$  $y_5 = |(m_4m_3m_2m_1)^{-1}m_5(x_5 - (y_4m_3m_2m_1 + y_3m_2m_1 + y_2m_1 + y_1))|$ m5  $(m_4m_3m_2m_1)^{-1}_{m_5} = (31*17*16*15)^{-1}_{7}$  $=|126480|^{-1}$  $126480 * k_4 = (1 \mod 7)$  $4 k_4 = (1 \mod 7)$ 

K<sub>4</sub>=2

## 4. REVERSE CONVERTER DESIGN FOR FIVE MODULI SET WITH PROPOSED CRT

In the proposed method the Chinese remainder theorem is used to design the reverse converter for the three, four and five moduli set. The CRT has low conversion delay and efficient architecture because of its parallel nature.

## 4.1 THEORETICAL CALCULATIONS: 4.1.1: 3 MODULI SET

Moduli set  $m = \{m_1, m_2, m_3\} = \{3, 4, 5\}$  and Residue set  $x = \{x_1, x_2, x_3\} = \{2, 3, 1\}$ The Chinese remainder theorem is given as  $X = |X_1M_1Y_1 + X_2M_2Y_2 + X_3M_3Y_3| \mod M \rightarrow (1)$ Where  $M=m_1*m_2*m_3$ M = 3\*4\*5 = 60Where  $M_i = M/m_i$  $M_1 = M/m_1 = 60/3 = 20$  $M_2 = M/m_2 = 60/4 = 15$  $M_3 = M/m_3 = 60/5 = 12$ Where  $\mathbf{Y}_{i} = |\mathbf{M}_{i}|^{-1} \min_{\mathbf{M}_{i}}$  $Y_1 = |M_1|^{-1} m_1 = |20|^{-1} 3$  $20 Y_1 = (1 \mod 3)$  $2 Y_1 = (1 \mod 3)$  $Y_1 = 2$ Similarly  $\dot{Y}_2 = |M_2|^{-1}{}_{m2} = |15|^{-1}{}_4 = 3$  $Y_3 = |M_3|^{-1}{}_m{}_3 = |12|^{-1}{}_5 = 3$ Substitute all values in equation (1)  $X = |X_1M_1Y_1 + X_2M_2Y_2 + X_3M_3Y_3| \text{ mod } M$  $X = |2*20*2+3*15*3+1*12*3| \mod 60$  $X = |251| \mod 60$ X=11

## 4.1.2: 4 MODULI SET

Moduli set m=  $\{m_1, m_2, m_3, m_3, m_4\} = \{5, 7, 8, 9\}$  and Residue set  $x = \{x_1, x_2, x_3, x_4\} = \{1, 2, 3, 4\}$ The Chinese remainder theorem is given as  $X = |X_1M_1Y_1 + X_2M_2Y_2 + X_3M_3Y_3 + X_4M_4Y_4| \mod M$ (1)Where  $M = m_1 * m_2 * m_3 * m_4$ M = 5\*7\*8\*9 = 2520Where  $M_i = M/m_i$  $M_1 = M/m_1 = 2520/5 = 504$  $M_2 = M/m_2 = 2520/7 = 360$  $M_3 = M/m_3 = 2520/8 = 315$  $M_4 = M/m_4 = 2520/9 = 280$ Where  $Y_i = |M_i|^{-1} m_i$  $Y_1 = |M_1|^{-1} m_1 = |504|^{-1} 5$ 504  $Y_1 = (1 \mod 5)$  $4 Y_1 = (1 \mod 5)$ 



## International Journal of Advanced Research in Computer and Communication Engineering ISO 3297:2007 Certified

Vol. 5, Issue 8, August 2016

 $\begin{array}{c} Y_1 = 4 \\ \text{Similarly } Y_2 = |M_2|^{-1}{}_{m2} = |360|^{-1}{}_7 = 5 \\ Y_3 = |M_3|^{-1}{}_{m3} = |315|^{-1}{}_8 = 3 \\ Y_4 = |M_4|^{-1}{}_{m4} = |280|^{-1}{}_9 = 1 \\ \text{Substitute all values in equation (1)} \\ X = |X_1M_1Y_1 + X_2M_2Y_2 + X_3M_3Y_3 + X_4M_4Y_4 \mid \text{mod } M \\ X = |1*504*4 + 2*360*5 + 3*315*3 + 4*280*1| \mod 2520 \\ X = |9571| \mod 2520 \\ X = 2011 \\ \end{array}$ 

## 4.1.3: 5 MODULI SET

Moduli set  $m = \{m_1, m_2, m_3, m_4, m_5\} = \{15, 16, 17, 31, 7\}$ Residue set  $x = \{x_1, x_2, x_3, x_4, x_5\} = \{7, 13, 4, 2, 3\}$ Chinese remainder theorem is given as

 $\begin{array}{l} X= \mid X_1M_1Y_1+X_2M_2Y_2+X_3M_3Y_3+X_4M_4Y_4+X_5M_5Y_5 \mid mod \\ M \rightarrow (1) \\ Where \ M=m_1*m_2*m_3*m_4*m_5 \\ M= 15*16*17*31*7=885360 \\ \\ Where \ M_i=M/m_i \\ M_1=M/m_1=885360/15=59024 \end{array}$ 

$$\begin{split} \mathbf{M}_{1} &= \mathbf{M}/\mathbf{M}_{1} &= 885360/15 = 59024 \\ \mathbf{M}_{2} &= \mathbf{M}/\mathbf{m}_{2} = 885360/16 = 55335 \\ \mathbf{M}_{3} &= \mathbf{M}/\mathbf{m}_{3} = 885360/17 = 52080 \\ \mathbf{M}_{4} &= \mathbf{M}/\mathbf{m}_{4} = 885360/31 = 28560 \\ \mathbf{M}_{5} &= \mathbf{M}/\mathbf{m}_{5} = 885360/7 = 126480 \\ \end{split}$$
 Where  $\mathbf{Y}_{i} &= |\mathbf{M}_{i}|^{-1} \mathbf{m}_{i} \\ \mathbf{Y}_{1} &= |\mathbf{M}_{i}|^{-1} \mathbf{m}_{i} = |59024|^{-1} 15 \\ 59024 \mathbf{Y}_{1} &= (1 \mod 15) \\ 14 \mathbf{Y}_{1} &= (1 \mod 15) \\ \mathbf{Y}_{1} &= 14 \\ \end{aligned}$  Similarly  $\mathbf{Y}_{2} &= |\mathbf{M}_{2}|^{-1} \mathbf{m}_{2} = |55335|^{-1} 16 = 7 \\ \mathbf{Y}_{3} &= |\mathbf{M}_{3}|^{-1} \mathbf{m}_{3} = |52080|^{-1} 17 = 2 \\ \mathbf{Y}_{4} &= |\mathbf{M}_{4}|^{-1} \mathbf{m}_{4} = |28560|^{-1} 31 = 7 \\ \mathbf{Y}_{5} &= |\mathbf{M}_{5}|^{-1} \mathbf{m}_{5} = |126480|^{-1} 7 = 2 \end{split}$ 

 $\begin{array}{l} \mbox{Substitute all values in equation (1)} \\ X = & |X_1M_1Y_1 + X_2M_2Y_2 + X_3M_3Y_3 + & X_4M_4Y_4 + X_5M_5Y_5 \mid \\ \mbox{mod } M \\ X = & |7*59024*14 + 13*55335*7 + 4*52080*2 \\ + & 2*28560*7 + 3*126480*2 \mid \mbox{mod } 885360 \\ X = & |12395197| \mbox{mod } 885360 \\ X = & |157 \\ \end{array}$ 

## 5. SIMULATION RESULTS

The proposed and existing reverse converter architectures are simulated and synthesized in Xilinx ISE Design Suite 14.7 version using Verilog HDL. The figure1 and 2, figure 3 and 4, and figure 5 and 6 shows the simulated waveforms of the reverse converter for three, four and five moduli set with MRC and CRT respectively. The table1 shows the performance analysis of the reverse converter design with different moduli sets.

The three moduli set is  $(2^{n}-1, 2^{n}, 2^{n}+1)$ . Here we take n=2, so the moduli set is  $\{3, 4, 5\}$  and residue set is  $\{2, 3, 1\}$ . The result is 11(1011).

Name	Value	1,999,995 ps	1,999,996 ps	1,999,997 ps	1,999,998 ps	1,999,999 ps
🕨 📑 x1(5:0)	000010			000010		
▶ 📑 x2[5:0]	000011			000011		
▶ 📑 x3[5:0]	000001			000001		
n[5:0]	000010			000010		
▶ 📑 z[11:0]	00000000101			000000001011		
▶ 🎼 m1[11:0]	00000000001			000000000011		
▶ 🎼 m2[11:0]	0000000010			000000000100		
▶ 🎼 m3[11:0]	00000000010			000000000101		
▶ 📑 k1[11:0]	00000110010			000001100100		
▶ 🎼 k2[11:0]	00000110010			000001100100		
▶ 🖏 y1[11:0]	00000000001			000000000010		
▶ 📑 y2[11:0]	00000000001			000000000011		
▶ 🚮 y3[11:0]	00000000000			00000000000000		
▶ 🚮 n1[11:0]	00000110001			000001100011		
▶ 📑 n2[11:0]	00000110001			000001100010		
🕨 📷 k4[11:0]	00000110001			000001100011		

Fig.1: MRC simulation results for three moduli set

Name	Value	2,999,995 ps  2,999,996 ps  2,999,997 ps  2,999,998 ps  2,999,999 ps
🕨 📑 n(3:0)	0010	0010
🕨 📑 x1[5:0]	000010	000010
🕨 📑 x2[5:0]	000011	000011
🕨 📑 x3[5:0]	000001	000001
🕨 📑 z[8:0]	000001011	000001011
🕨 📑 m[31:0]	00000000000	000000000000000000000000000000000000000
🕨 📑 m1[31:0]	00000000000	000000000000000000000000000000000000000
▶ 📑 m2[31:0]	00000000000	000000000000000000000000000000000000000
🕨 📑 m3[31:0]	00000000000	000000000000000000000000000000000000000
🕨 📑 m4[31:0]	00000000000	000000000000000000000000000000000000000
🕨 📑 m5[31:0]	00000000000	000000000000000000000000000000000000000
🕨 📑 m6[31:0]	00000000000	000000000000000000000000000000000000000
🕨 📑 k1[31:0]	00000000000	000000000000000000000000000000000000000
🕨 📑 k2[31:0]	00000000000	000000000000000000000000000000000000000
🕨 📑 k3[31:0]	00000000000	000000000000000000000000000000000000000
🕨 📑 y1[31:0]	00000000000	000000000000000000000000000000000000000
		X1: 3,000,000 ps

Fig.2: CRT simulation results for three moduli set.

The four moduli set is  $(2^{n-1}+1, 2^n-1, 2^n, 2^n+1)$ . Here we take n=3, so the moduli set is {5, 7, 8, 9} and residue set is {1, 2, 3, 4}. The result is 2011(1111011011).

					1,999,998 ps		
Name	Value	1,999,995 ps	1,999,996 ps	1,999,997 ps	1,999,998 ps	1,999,999 ps	
▶ 📑 x1(5:0)	000001			000001			
▶ 📑 x2[5:0]	000010			000010			
▶ 📑 x3[5:0]	000011			000011			
▶ 📑 x4[5:0]	000100			000100			
🕨 📑 n(5:0)	000011			000011			
▶ 📑 z[11:0]	01111101101			011111011011			
🕨 🚮 k1(11:0)	00000000100			000000001000			
▶ 📑 k2[11:0]	00000000100			000000001001			
🕨 📑 k3(11:0)	00000000101			000000001010			
🕨 📷 y1[11:0]	0000000000			0000000000001			
▶ 📷 y2[11:0]	00000000001			000000000011			
▶ 🚮 y3[11:0]	00000000000			0000000000001			
▶ 📷 y4[11:0]	0000000011			000000000111			
▶ 🖏 n1[11:0]	00000000001			000000000011			
▶ 📷 n2[11:0]	00000000001			000000000011			
▶ 🚮 n3[11:0]	00000000000			000000000000000000000000000000000000000			

Fig.3: MRC simulation results for four moduli set

		1,999,999 ps
Name	Value	1,999,995 ps  1,999,996 ps  1,999,997 ps  1,999,998 ps 1,999,999 ps
🕨 📑 n(6:0)	0000011	0000011
🕨 📑 x1(6:0)	0000001	0000001
▶ 📑 x2[6:0]	0000010	0000010
▶ 📑 x3(6:0)	0000011	0000011
🕨 📑 x4[6:0]	0000100	0000100
▶ 📷 z[31:0]	0000000000	000000000000000000000000000000000000000
🕨 🚮 m(31:0)	0000000000	000000000000000000000000000000000000000
🕨 📷 m1(31:0)	00000000000	000000000000000000000000000000000000000
▶ 📑 m2[31:0]	00000000000	000000000000000000000000000000000000000
🕨 📷 m3(31:0)	0000000000	000000000000000000000000000000000000000
🕨 📷 m4[31:0]	00000000000	000000000000000000000000000000000000000
🕨 📷 m5[31:0]	00000000000	000000000000000000000000000000000000000
🕨 📷 m6(31:0)	00000000000	000000000000000000000000000000000000000
🕨 黬 m7[31:0]	00000000000	000000000000000000000000000000000000000
🕨 📷 m8[31:0]	00000000000	000000000000000000000000000000000000000
🕨 📑 y1[31:0]	00000000000	000000000000000000000000000000000000000

Fig.4: CRT simulation results for four moduli set.



## International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified

Vol. 5, Issue 8, August 2016

Here we take n=4.So the five moduli set is  $(2^{n}-1, 2^{n}, 2^{n}+1,$  $2^{n+1}-1$ ,  $2^{n-1}-1$ ) = (15, 16, 17, 31, 7) and the residue set is (7, 13, 4, 2, 3) .The result is 157 (10011101)

ame	Value	1,999,995 ps	1,999,996 ps	1,999,997 ps	1,999,998 ps	1,999,999 ps
📲 x1[10:0]	00000000111			0000000111		
📑 x2[10:0]	00000001101			00000001101		
📑 x3[10:0]	00000000100			0000000100		
📑 x4[10:0]	00000000010			00000000010		
📲 x5[10:0]	00000000011			00000000011		
📑 n(10:0)	00000000100			0000000100		
📲 z[25:0]	00000000000		000000	0000000000010011	01	
🚮 m1[25:0]	00000000000		000000	000000000000000000000000000000000000000	111	
🚮 m2[25:0]	00000000000		000000	000000000000000000000000000000000000000	000	
🚮 m3[25:0]	00000000000		000000	000000000000000000000000000000000000000	01	
🚮 m4[25:0]	00000000000		000000	00000000000000011	11	
🚮 m5[25:0]	00000000000		000000	000000000000000000000000000000000000000	111	
🚮 k1[25:0]	00000000000		000000	000000000000000000000000000000000000000	001	
🚮 k2[25:0]	00000000000		000000	000000000000000000000000000000000000000	010	
🚮 k3[25:0]	00000000000		000000	000000000000000000000000000000000000000	000	
🚮 k10[25:0]	0000000000		000000	000000000000000000000000000000000000000	000	

Fig.5: MRC simulation results for five moduli set

						1,999,999 ps	
Name	Value	1,999,995 ps	1,999,996 ps	1,999,997 ps	1,999,998 ps	1,999,999 ps	2,000,000 p
🕨 🕌 n(9:0)	0000000100			0000000100			
🕨 🕌 x1(9:0)	0000000111			0000000111			
🕨 🕌 x2(9:0)	0000001101			0000001101			0
🕨 🕌 x3[9:0]	0000000100			0000000100			
🕨 🕌 x4(9:0)	0000000010			0000000010			
🕨 🕌 x5(9:0)	0000000011			0000000011			
🕨 📑 z[31:0]	0000000000		000000000	000000000000000000000000000000000000000	11101		
🕨 👹 m(31:0)	00000000000		000000000	0011011000001001	10000		D
🕨 👹 m1(31:0)	00000000000		000000000	000000000000000000000000000000000000000	01111		5
🕨 👹 m2(31:0)	00000000000		000000000	000000000000000000000000000000000000000	10000		
🕨 👹 m3(31:0)	00000000000		000000000	000000000000000000000000000000000000000	10001		0
🕨 👹 m4(31:0)	00000000000		000000000	000000000000000000000000000000000000000	11111		D
🕨 👹 m5(31:0)	00000000000		000000000	000000000000000000000000000000000000000	00111		
▶ 👹 m6[31:0]	00000000000		000000000	0000001110011010	10000		D
🕨 👹 m7(31:0)	00000000000		000000000	0000001101100000	00111		
🕨 👹 m8(31:0)	00000000000		00000000	0000001100101101	10000		

Fig.6: CRT simulation results for five moduli set

The proposed reverse converter design for five moduli set using CRT is efficient than the existing MRC reverse converter design.

Moduli set	Delay	/ (ns)	Dynamic Range (bits)
	MRC CRT		
5Moduli	638.60	186.71	5n-1
4Moduli	223.21	175.59	4n
3Moduli	185.65	171.12	3n

Table 1: Performance Analysis

## 6. CONCLUSION

This work aims to build an efficient Reverse converter for five moduli set residue number system, with high dynamic range to increases the parallelism.

The proposed method has less conversion delay (high speed) than the existing method. It has high dynamic range up to 5n-1.The performance analysis as shown in the table Institute of Technology and Sciences, Rajampeta. His 1.

#### ACKNOWLEDGMENT

This work is sponsored and supported by Annamacharya Institute of Technology and Sciences: Rajampet. My sincere thanks to my guide B. Sekhar and my Head of the Department B. Abdul Rahim for their valuable suggestions.

#### REFERENCES

- [1] R.I.Tanaka and N.S.Szabo,"Residue Arithmetic and its Applications to Computer Technology". New York, McGraw Hill, 1967.
- M. A. Soderstrand, W.K, Jenkins, G.A. Jullien and F.J. Taylor, [2] "Residue Number System Arithmetic: Modern Applications in Digital Signal Processing". New York: IEEE Press, 1986.
- A. Omondi and B. Premkumar, "Residue Number System: Theory [3] and Implementation, "Imperial College Press 2007, ISBN 978-1-86094-866-4.
- S.Palnitkar, "Verilog HDL- A Guide to Digital Design and [4] Synthesis," Prentice Hall PTR, ISBN: 0-13-044911-3.
- A. Mohan, "Efficient Design of Binary to RNS Converters," [5] Journal of Circuits and Systems, 1999.
- [6] A. Skavantzos and M. Abdallah, "Implementation issues of the two level residue number system with pairs of conjugate moduli," IEEE Trans. Signal Process., Mar. 1999.
- M.Bhardwaj, T.Srikanthan, and C. T. Clarke, "A reverse converter for the 4-moduli superset  $\{2^{n-1}, 2^n, 2^{n+1}, 2^{n+1}, 2^{n+1}+1\}$ ," in Proc. 14<sup>th</sup> IEEE [7] Symp. Computer Arithmetic, Australia, Apr. 1999
- [8] T.Srikanthan, B.Cao and C.H.Chang, "Efficient reverse converters for the 4-moduli supersets {2n-1,2n,2n+1,2n+1-1} and {2n-1,2n,2n+1,2n-1-1}" Proc .IEE Comput. Digit. Tech.
- [9] A. Skavantzos, "An Efficient Residue to Weighted Converter for a New Residue Number System," in Proc. 8th Great Lakes Symp. VLSI, New Orleans, LA, Feb. 1998
- [10] T.Stouraitis and A. Skavantzos, "Grouped-moduli Residue Number Systems for Fast Signal Processing," in Proc. Int. Symp. Circuits Syst., Jun. 1999.
- [11] A.Hiasat, "Efficient Residue to Binary Converter," Proc. IEE Comput. Digit. Tech., Jan. 2003.

## **BIOGRAPHIES**



Y. Ayyavaru Reddy received the B.Tech degree in Electronics Communication and Engineering from Sir Vishveshwaraiah Institute of Science and Technology, Madanapalli in 2014. He is pursing M.Tech under the

specialization of VLSI system Design in Annamacharya Institute of Technology and Sciences, Rajampeta. His research areas are VLSI and Signal processing.



B. Sekhar received the B.Tech degree in Electronics and Communication Engineering from Rajeev Gandhi Memorial College of Engineering and Technology, Nandyal in 2007. He received M.Tech degree in VLSI system

Design from Annamacharya Institute of Technology and Sciences, Rajampeta. He is pursing PhD from JNTU, Kakinada. He is currently working as an Assistant processor for the Department of ECE at Annamacharya research areas are VLSI & Signal processing.