ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Special Issue 3, April 2017

VLSI Architecture of Matrix Based RNS Backward Converter

U.M.Sreelekha[1], B.Sarala[2]

UG Student, Department of ECE, Sri Venkateswara College of Engineering, Sriperumbudur, Chennai, India

Assistant Professor, Department of ECE, Sri Venkateswara College of Engineering, Sriperumbudur, Chennai, India

ABSTRACT: Residue Number system is an important research area for the past few years. RNS is an unconventional number system unlike the weighted number system. RNS is nothing but representing larger set of numbers by a small set of integers. These integers are nothing but the residues. RNS avoids carry propagation so that, It can be extensively used for faster and parallel operations which eventually increases the efficiency of the system. RNS processer performs three processes: forward conversion, arithmetic operation and backward conversion. In this paper, an efficient way of performing backward conversion is adopted.

KEYWORDS: Forward conversion, Reverse conversion, Residue number system.

I. INTRODUCTION

Residue Number System is based on a relation called congruence relation. This relation is defined as follows. Two integers a and b are said to be congruent modulo m if m exactly divides the difference of a and b. Among the process of RNS processes, backward conversion is considered to be complicated and cost overhead. There are some methods or algorithms to implement backward conversion such as Chinese remainder theorem and mixed radix conversion.

This paper focuses on implementing mixed matrix method for RNS, especially backward conversion which provides an area efficient system. When RNS is used in practical applications such as communication engineering, fault tolerance, error detection and correction codes, cryptography etc., it must deploy very less area. Then it can be declared as an area efficient method. In this paper, Chinese remainder theorem and adopted mixed matrix method are compared in terms of area i.e. number of adders/ subtractors and multipliers.

II.CHINESE REMAINDER THEOREM

Chinese remainder theorem (CRT) is an existing theorem which is implemented in cryptographic application. Chinese remainder theorem is based on the following statement: if one knows the remainder of the division of an integer n by several integers(divisors),then one can find the remainder of the division of integer n by the product of those integers(divisors), provided those integers are pairwise coprime. As stated above, backward conversion is a critical stage at the receiver end. So, the following explains the process of performing the backward conversion as per CRT.

III.PROCESS OF CHINESE REMAINDER THEOREM (BACKWARD CONVERSION)

This method is based on an algorithm which goes as follows with an example. Consider 2 decimal numbers (10+8). Consider the prime moduli set as (2, 3, 5). By performing the mod operation for 10 with moduli set as above, we get the "residue" set as (0, 1, 0). Similarly for number 8, it gives (0, 2, 3). This is the "forward conversion" process. Now performing the addition for both the residue sets we get (0, 3, 3). The main process in this project is the "backward conversion" which converts the resulting residue set to the decimal number required. The number is found as follows.

x= (0 mod 2)…………… (1)
x= (3 mod 3)…………… (2)
x= (3 mod 5)…………… (3)

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

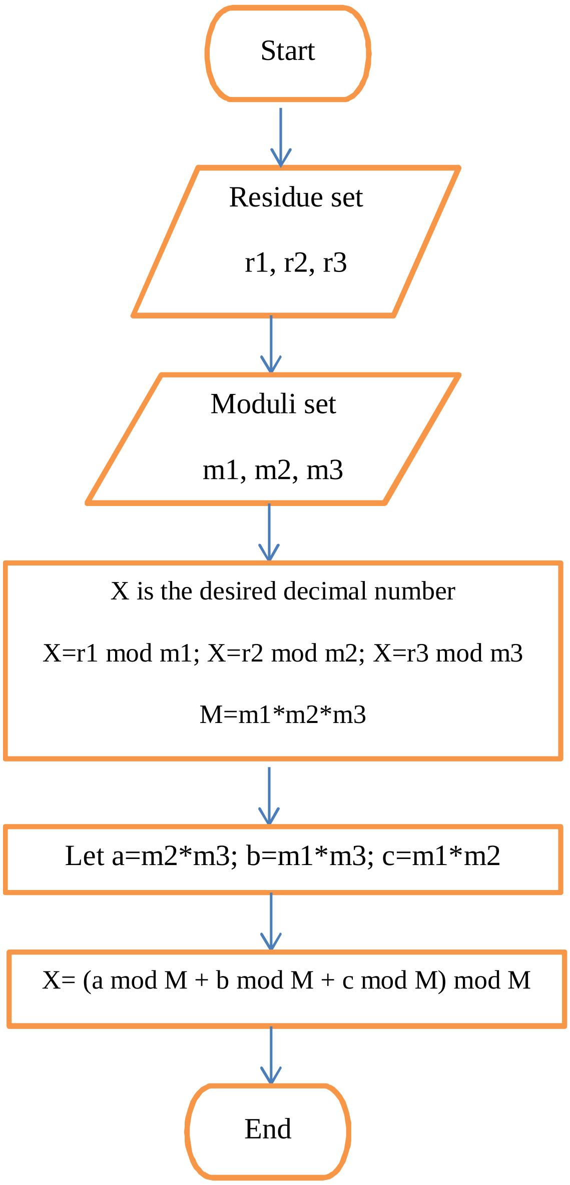
Vol. 5, Special Issue 3, April 2017

Multiplying the prime moduli set (2, 3, 5), we get 30.For the first location, the multiplicative term is 15. For the second location, it is 10 and for the third location, it is 6. By using all these equations, the main equation from which the desired number is obtained is given as follows.

x= (15 mod 30 + 10 mod 30 + 6 mod 30) mod 30 .

Multiplying the respective location's multiplicative terms with their respective residues, then accumulating all of them and taking the modulus of the accumulated number with the moduli set multiplicative term, the number is obtained. x= (15*0 + 10*3 + 6*3) mod 30. x= 48 mod 30.which is equal to 18. Therefore 18 is the required decimal number.

IV. BLOCK DIAGRAM OF CRT



ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Special Issue 3, April 2017

V. MIXED MATRIX METHOD

The mixed matrix method which is adopted in this paper, proves to be an area efficient method in terms of number of adders/subtractors and multipliers. The process of performing mixed matrix method is given as follows.
Consider the residue set as “r” and moduli set as “m”. The number to be found is X. Let the residue set be r= {r1, r2, r3} and prime moduli set be as m= {m1, m2, m3}. For the first location,

$$X\text{-}r1 = \begin{pmatrix} (r1-r1)_{m1} \\ (r2-r1)_{m2} \\ (r3-r1)_{m3} \end{pmatrix} = \begin{pmatrix} \text{residue1} \\ \text{residue2} \\ \text{residue3} \end{pmatrix}$$

Consider a variable J2 where X-r1-J2 is used in the second location. J2=K2*m1 if **(residue 2- J2) mod m2=0.**For the second location,

$$X\text{-}r1\text{-}J2 = \begin{pmatrix} (\text{residue1}-J2) \\ (\text{residue2}-J2) \\ (\text{residue3}-J2) \end{pmatrix} \begin{matrix} m1 \\ m2 \\ m3 \end{matrix} = \begin{pmatrix} \text{residue4} \\ \text{residue5} \\ \text{residue6} \end{pmatrix}$$

Consider a variable J3 where X-r1-J2-J3 is used in the second location. J3=K3*m2 if **(residue 6- J3) mod m3=0**.

$$X\text{-}r1\text{-}J2\text{-}J3 = \begin{pmatrix} (\text{residue4}-J3) \\ (\text{residue5}-J3) \\ (\text{residue6}-J3) \end{pmatrix} \begin{matrix} m1 \\ m2 \\ m3 \end{matrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix}$$

Therefore, the required decimal number is X=r1+J2+J3.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

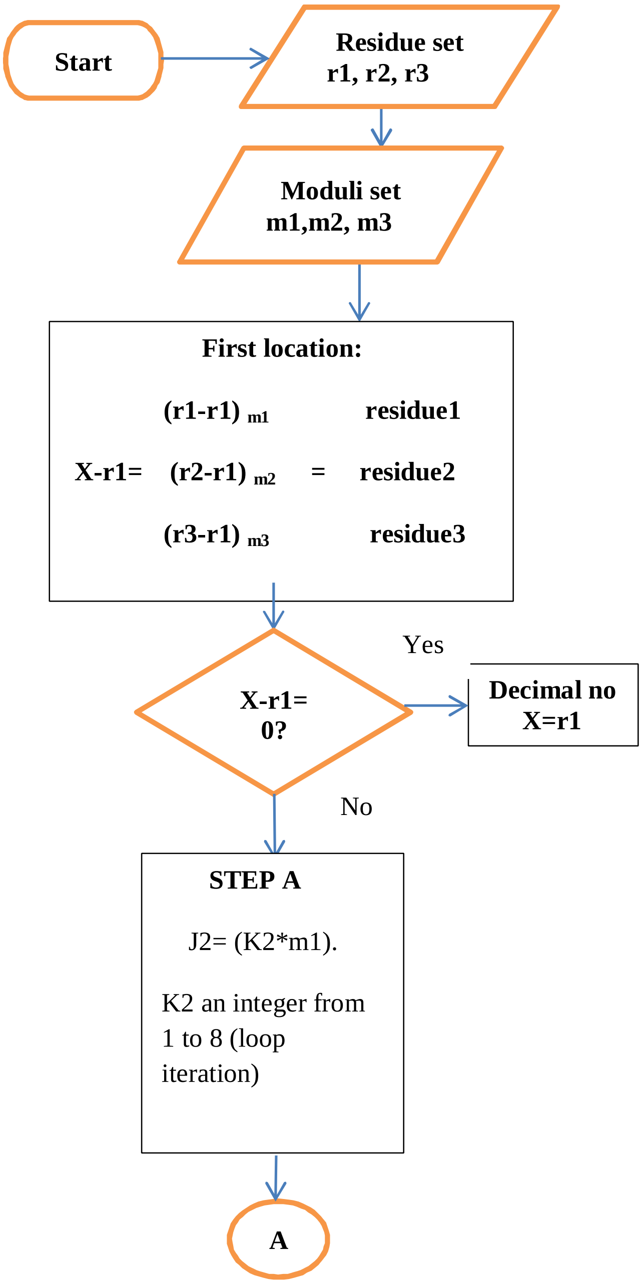
International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Special Issue 3, April 2017

VI. BLOCK DIAGRAM



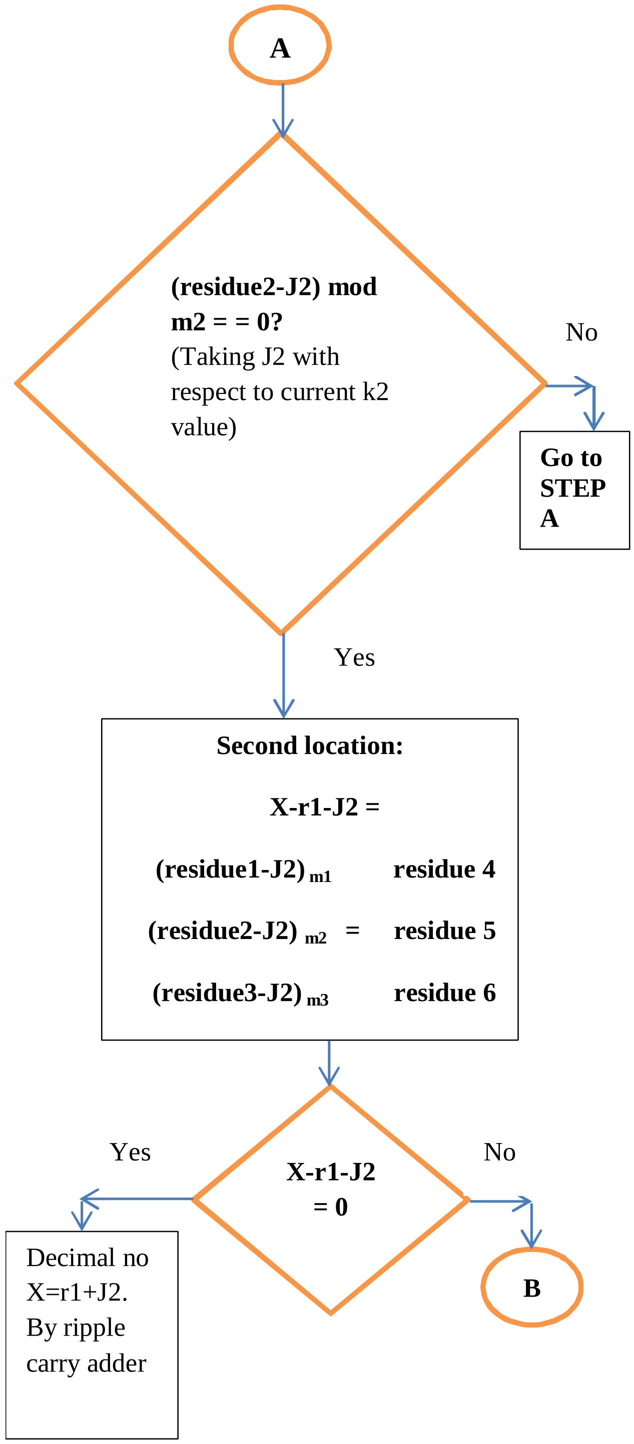
ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Special Issue 3, April 2017



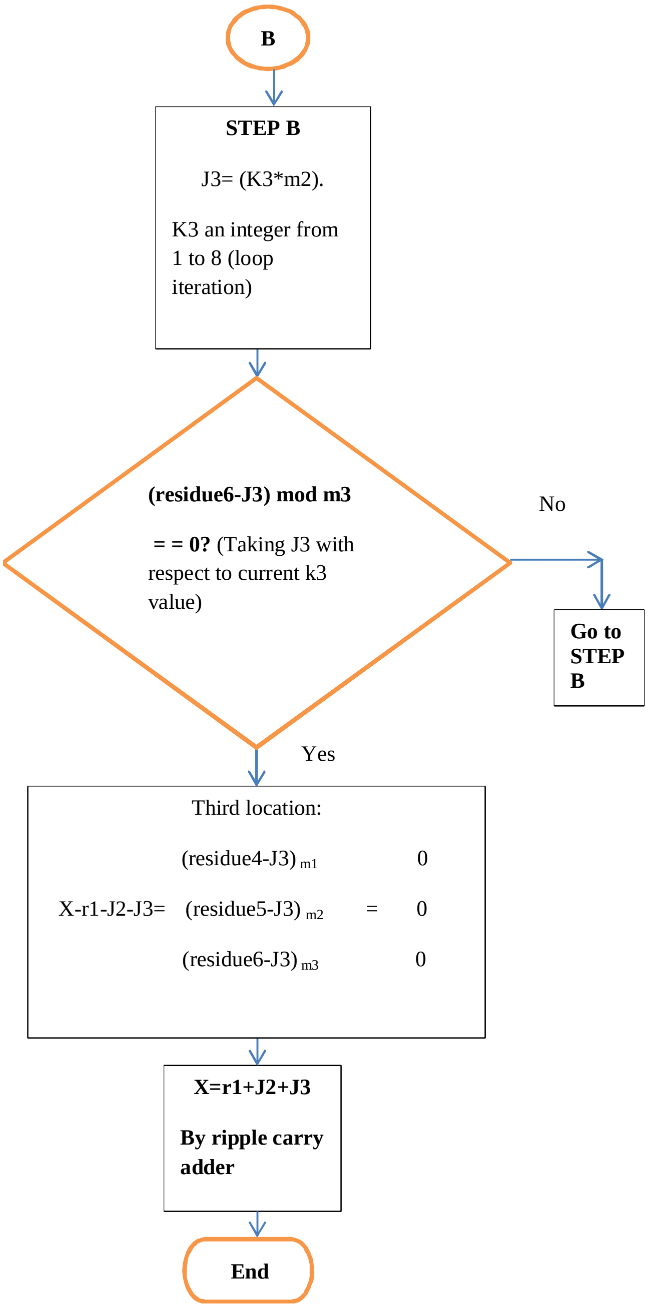
ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Special Issue 3, April 2017



VII. EXAMPLE OF MIXED MATRIX METHOD

Consider the residue set as “r” and moduli set as “m”. The number to be found is X. Let the residue set be r= { 0,2,3 } and prime moduli set be as m={ 2,3,5} where r1=0,r2=2,r3=3 and m1=2,m2=3,m3=5. For the first location,

X-r1= X-0 = $(r1\text{-}r1)_2$ = $(0\text{-}0)_2$ = 0
$(r2\text{-}r1)_3$ $(2\text{-}0)_3$ 2
$(r3\text{-}r1)_5$ $(3\text{-}0)_5$ 3

Therefore, 0 = residue 1
2 residue 2
3 residue 3

Consider a variable J2 where X-0-J2 is used in the second location. J2=K2*m1 if **(residue 2- J2) mod m2=0**. Here, J2=K2*2 if (2-J2) mod 3=0. By checking the condition, the value of K2 is 1. Therefore, J2=2. For the second location,

X-r1-J2 = X-0-2 = $(residue1\text{-}J2)_2$ = $(0\text{-}2)_2$
$(residue2\text{-}J2)_3$ $(2\text{-}2)_3$
$(residue3\text{-}J2)_5$ $(3\text{-}2)_5$

Therefore, = 0 = residue 4
0 residue 5
1 residue 6

Consider a variable J3 where X-0-2-J3 is used in the second location. J3=K3*m2 if **(residue 6- J3) mod m3=0**. Here, J3=K3*3 if (1-J3) mod 5=0. By checking the condition, the value of K3 is 2. Therefore, J3=6. For third location,

$(residue4\text{-}J3)_2$
X-r1-J2-J3= X-0-2-6 = $(residue5\text{-}J3)_3$
$(residue6\text{-}J3)_5$

Therefore, $(0\text{-}6)_2$ = 0
$(0\text{-}6)_3$ 0
$(1\text{-}6)_5$ 0

Therefore, X-0-2-6=0, which means X=0+2+6. **X=8 is the required decimal number.**

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

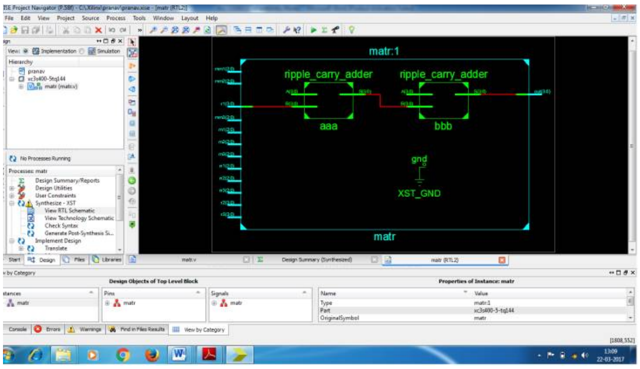
(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Special Issue 3, April 2017

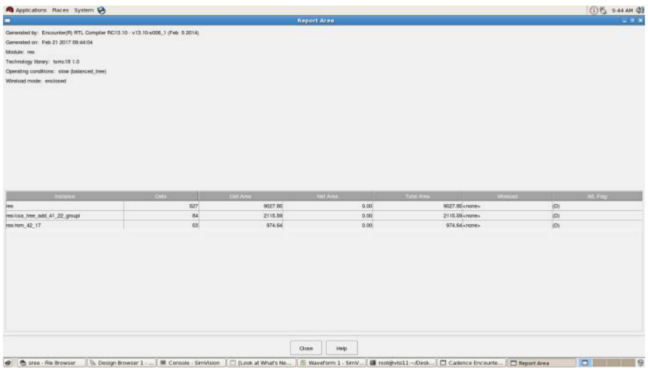
VIII. VLSI ARCHITECTURE FOR MATRIX BASED RNS BACKWARD CONVERTER

This architecture includes ripple carry adder becausethe least power dissipation occurs for ripple carry adder with a small area occupation. Moreover the design layout is also simple.



VIII. CADENCE RESULTS

The CRT method when analysed using cadence, the area occupied is obtained as 9027.85μm^2.



The comparison of the number of adders/ subtractors and multipliers between CRT and mixed matrix method is given as follows.

METHOD	ADDERS / SUBTRACTORS	MULTIPLIERS
CRT	33	7
MIXED MATRIX	14	3

The percentage decrease of number of adders/subtractors from CRT to mixed matrix method is 57.57% and for number of multipliers is 57.14%.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Special Issue 3, April 2017

IX. CONCLUSION

Hence, mixed matrix method is an area efficient method to perform backward conversion. By comparing the above table, the mixed matrix method is superior to Chinese remainder theorem in terms of the usage of number of adders/ subtractors and multipliers. Thus when this method is used to perform backward conversion in applications such as cryptography, secure data transmission will take place. It provides a faster operation in computer arithmetic as well.

REFERENCES

1. Bhavana Rayapudi, I.B.K Raju, Gnaneshwara Chary, Pranay Deekonda, Prashanth Ummadisettia,"AN EFFICIENT VLSI ARCHITECTURE FOR MATRIX BASED RNS BACKWARD CONVERTER" IEEE International Conference on Computer Modelling and Security, Procedia Computer Science, pp 85 (2016) 271 – 277.
2. Kazeem Alagbe Gbolagade and Sorin Dan Cotofana,"GENERALISED MATRIX METHOD FOR EFFICIENT RESIDUE TO DECIMAL CONVERSION", IEEE Asia Pacific Conference, 2008.
3. R.Karmugilan, Dr. R. Vijayabhasker "DESIGN AND IMPLEMENTATION OF RESIDUE NUMBER SYSTEM USING HIGH SPEED REVERSE CONVERTER", International Journal of Advanced Science and Engineering Research, Volume: 1, Issue: 1, June 2016.
4. Fred J. Taylor, "RESIDUE ARITHMETIC: A TUTORIAL WITH EXAMPLES", IEEE Transaction On Computer, pp. 50~62, May 1984.
5. Yuck Wang, "RESIDUE–TO-BINARY CONVERTERS BASED ON NEW CHINESE REMAINDER THEOREM,"IEEE Transactions On Circuits And Systems- II:Analog And Digital Signal Processing,Vol.47,No.3,March 2000.