Design of RNS Based Addition Subtraction and Multiplication Units

N Vivek[1], K Anusudha[2]

[1] Department of Electronic Engineering, Pondicherry University, Pondicherry, India
[2] Department of Electronic Engineering, Pondicherry University, Pondicherry, India

***Abstract*— Residue number systems have gained significant importance in the field of high-speed digital signal processing due to their carry-free nature and speed-up provided by parallelism. The cynical aspect in the application of RNS is the selection of the moduli set and the design of the conversion units. In the residue number system, a set of moduli which are independent of each other is given. An integer is represented by the residue of each modulus and the arithmetic operations are based on the residues individually. The arithmetic operations based on residue number system can be performed on various moduli independently to avoid the carry obtained in addition, subtraction and multiplication, which is usually time consuming. Thus, the comparison and division are more complicated and the fraction number computation is immured. In this paper, work is done by the residues of the number and performed Addition, Subtraction and Multiplication are performed which shows more advantages of Carry Free nature. Performance of RNS based Addition, subtraction and Multiplication Units has been implemented for modulo set {2^n -1, 2^n , 2^n+1} for n=2,3 with the targeted device of Spartan 3E using hardware description language called Verilog and synthesized in Xilinx ISE 13.2.**

***Keywords*— Residue Number System (RNS), New Chinese Remainder Theorem (NCRT), Multioperand Modular Adder (MOMA), Mixed Radix Theorem (MRT), Chinese Remainder Theorem(CRT),Carry Save Adder(CSA).**

I INTRODUCTION

Residue Number System is a mathematical idea from Sun Tsu Suan-Ching (Master Sun's Arithmetic Manual) in the 4th century AD from Chinese remainder theorem of modular arithmetic for its operation.

There has been interest in Residue Number System (RNS) arithmetic as a basis for computational hardware since the 1950's.Due to its special features, the Residue Number System has many applications in arithmetic functions such as Digital Signal Processing, Digital Filtering, Coding, RSA ciphering system, Digital communications, Ad-hoc network, storing and retrieving information, Error detection and Correction, and fault tolerant systems [11].

The main reasons for the interests are the inherent properties of RNS such as the parallelism, modularity, fault tolerance and carry free operations. The advantages offered by this VLSI technology have added a new dimension in the implementation of RNS-based architectures. Several high-speed VLSI special purpose digital signal processors have been successfully implemented.

A residue number system (RNS) represents a large integer using a set of smaller integers, so that computation may be performed more efficiently. The main objective of the project is to reduce complexity in addition, subtraction and multiplication for large integers using the RNS technique, and this RNS is mainly used in cryptography as the moduli used as cipher (key) for both encryption and decryption.

This paper is organized as follows; Section II explains the existing model of the RNS for Filter application and section III explains the proposed model for Addition, Subtraction and Multiplication Unit with Forward and Reverse Conversion with MOMA circuit. Simulation & Results are analyzed in the section IV, Section V with the conclusion.

II. EXISTING RNS MODEL FOR FILTER DESIGN

Figure1, depicts a basic N-Tap filter, where

$$y(n) = a_0x_0 + a_1x_1 + a_2x_2 \dots \dots + a_{N-1}x_{N-1} \dots \quad (1)$$

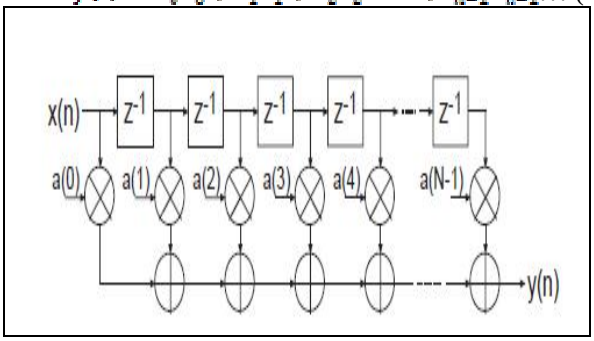

Figure 1 Basic FIR filter (N-tap)

Where,

x[n] is the input signal,
y[n] is the output signal,
$a_i$is the filter coefficients.

For FIR Filter of N order filter has

- Coefficients N+1
- Multipliers N+1
- Adders N

The 3 main blocks of RNS model are:

- Forward Conversion
- Channels (moduli)
- Reverse Conversion

Basic block diagram of RNS Model, is shown in Figure 2

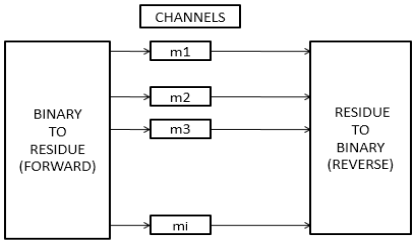

Figure 2: RNS MODEL

A.FORWARD CONVERSION

The forward conversion stage is of paramount importance as it is considered as an overhead in the overall RNS. Forward converters are usually classified into two categories based on the moduli used. The first category includes forward converters based on arbitrary moduli-sets. These converters are regularly built using Look Up Tables (LUTS) which consists of ROM's. The second category includes forward converters based on special moduli-sets. The use of these special moduli-sets simplifies the forward conversion algorithms and architectures.

Usually, the special moduli-sets are referred to as low-cost moduli-sets. A typical architecture for the implementation of a forward converter from binary to RNS representation using the special moduli-set is shown in Figure 3. One way of implementing a residue adder for modulo 'm' structure is composed of one n-bit adder among various ways [6].

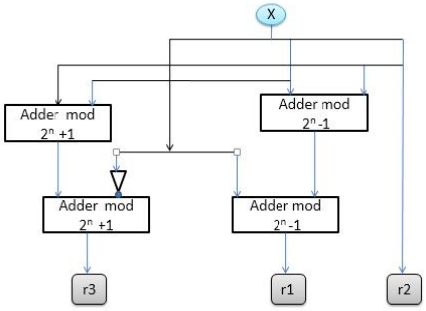

Figure 3: Forward conversion

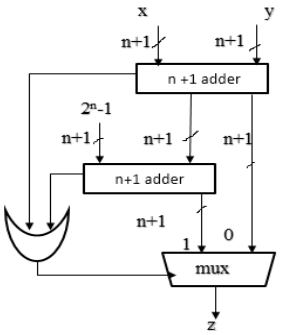

Fig. 4

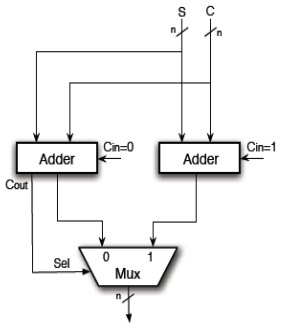

Fig.5

Figure 4 & 5: for 2^n-,2^n+1

B. CHANNELS

The Standard channels in RNS are three moduli i.e., {2^n-1, 2^n, 2^n+1} in which n describes the way of splitting the decimal value of 'X' we consider in Figure 2.

One of the most important considerations while designing RNS system is choice of selecting moduli set. The Choice of moduli affects the complexity of Forward and Reverse converters as well as RNS arithmetic Circuits [11]. Unbalanced and moduli-sets lead to uneven architectures, in which the role of largest moduli, with respect to both cost and performances, is excessively dominant. An example of a moduli-set with good balanced is 2^n-1, 2^n, 2^n+1 [7].

C. REVERSE CONVERSION

Converting residue number to binary number is called reverse conversion. Reverse conversion algorithms are classified into 3 types:

- Chinese Remainder Theorem (CRT)
- New Chinese Remainder Theorem (NCRT)
- Mixed Radix Theorem (MRT)

The new Chinese Remainder Theorems (NCRT) makes the computation faster and efficient without any extra overheads. A new high-speed ROM-less residue-to binary converter for the three moduli residue number system of the form {2" - 1, 2", 2" + 1} is used. Unlike any other converter, its delay includes the time of only one 1's complement addition of two 2n-bit numbers which is only 2/3 of the binary range of the RNS equal to as 3n. Thus, it is potentially the fastest known residue-to-binary converter [12].

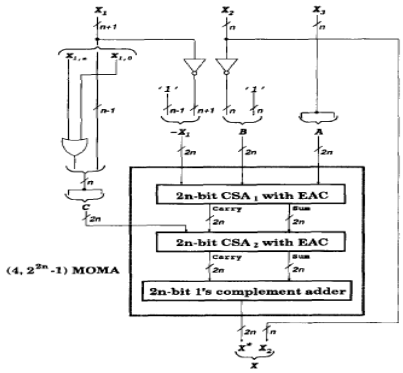

Figure 6 :Block Diagram for Reverse Convertor(New Chinese Remainder Theorem)

Multioperand Modular adders is an efficient architecture involving tree of CSA's with EAC as shown in Figure7.The Modulo Wallace tree is known to be regular than the binary Wallace-tree, therefore outputs need not to left shifted before given to the next stage in the 2^n-1[13].

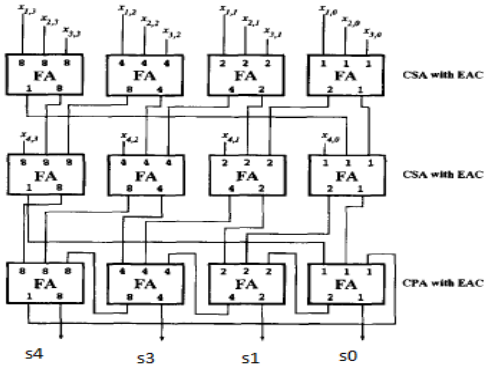

Figure 7: Block Diagram of MOMA

III. PROPOSED MODEL

The proposed structure is implementation of Addition, Subtraction and Multiplication Units in Residue Number System for order n=2 &3 is shown as Figure 8

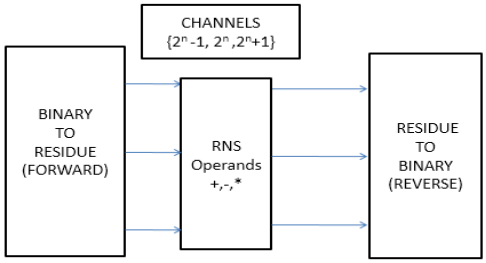

Figure 8: Block Diagram of Proposed Model

The basic formula for calculating Forward Conversion in RNS is

$$r1=|\mathbf{B1+B2+B3}|2^n-1 \quad \dots (2)$$

$$r2=\mathbf{B3} \quad \dots (3)$$

$$r3=|\mathbf{B1-B2+B3}|2^n+1 \quad \dots (4)$$

Algorithms for New Chinese Reminder Theorem:

Let the three residues be denoted **as** X1, X2, and X3. MSB are given first the decimal value of X and it can be computed as

$$A=(X_{3,0}, X_{3,n-1}\dots X_{3,1}, X_{3,0}, X_{3,n-1}\dots X_{3,1}) \quad \dots (5)$$

$$B=(\sim(X_{2,n-1}\dots X_{2,1}, X_{2,0}), 1, 1\dots..1) \quad \dots (6)$$

$$C=(b_0, X_{1,n-1}\dots X_{1,1}, b0, X_{1,n-1}\dots X_{1,1}) \quad \dots (7)$$

$$b0=X_{1,0}\,\&\,X_{1,n} \quad \dots (8)$$

$$Y=|A+B+C-X|2^{2n}-1 \quad \dots (9)$$

$$X=Y+X2 \quad \dots (10)$$

In the proposed model, the implementation of RNS based addition, subtraction and multiplication Units which are based on the Properties of RNS [4].

If the given moduli are m1, m2, m3…… m_N, X=(x1, x2, x3...x_N) and Y= (y1, y2,…,y_N)

Property 1:

$x_i=|x|_{mi}$ and $y_i=|Y|_{mi}$, then addition may be defined as X+Y=Z by

$$X+Y=(x1, x2\dots X_N) + (y1, y2, y3\dots y_N)$$
$$= (z1, z2, z3\dots Z_N)$$
$$=Z$$

Property 2:

$x_i=|x|_{mi}$ and $y_i=|Y|_{mi}$, then Subtraction may be defined as X-Y=Z by

$$X*Y=(x1, x2\dots X_N) + (m1-y1, m2-y2, m3-y3\dots m_N-y_N)$$
$$= (z1, z2, z3\dots Z_N)$$
$$=Z$$

Property 3:

$x_i=|x|_{mi}$ and $y_i=|Y|_{mi}$, then Multiplication may be defined as X*Y=Z by

$$X*Y=(x1, x2\dots X_N)*(y1, y2, y3\dots y_N)$$
$$= (z1, z2, z3\dots Z_N)$$
$$=Z$$

Here the New Chinese Reminder Theorem is considered due the less complexity compared with Mixed Radix Theorem.

Consider the Example :RNS Number x=(1,2,3,4) given moduli set as (3,5,7,11) using MRT

$$X=(a_1+a_2P_1+a3P_1P_2+a4P_1P_2P_3) \quad \dots (11)$$

Using equation (11) as follows

$$X=(a_1+a_2P_1+a_3P_1P_2+a_4P_1P_2P_3)$$
$$|1/P_1|_{P_2}=2,\quad |1/P_1|_{P_3}=5,\quad |1/P_2|_{P_3}=3$$
$$|1/P_1|_{P_4}=4,\quad |1/P_2|_{P_4}=9,\quad |1/P_3|_{P_4}=8$$
$$a_1=x_1=1$$
$$a_2=(2-1)*|1/P_1|_{P_2}=2$$
$$a_3=[(x_3-a_1)|1/P_1|_{P_3}-a_2]|1/P_2|_{P_3} \bmod P_3$$
$$=[(3-1)*5-2]*\bmod P_3=8*3 \bmod 7=3$$
$$a_4=\{[(x_4-a_1)|1/P_1|_{P_4}-a_2]|1/P_2|_{P_4}-a_3\}|1/P_3|_{P_4} \bmod P_4$$
$$=\{[(4-1)*4-2]*9-3\}*8 \bmod P_4$$
$$=87*8 \bmod 11=3$$
$$X=(1+2*3+3*3*5+3*3*5*7)=367$$

IV.SIMULATION RESULTS & RESULT ANALYSIS

The Top block of RNS based Adder, subtractor and Multiplication Units Consists of two opernand as inputs of which are in bit size of 6 and 9 bit and corresponding input order 'n' i.e, n=2 and n=3.

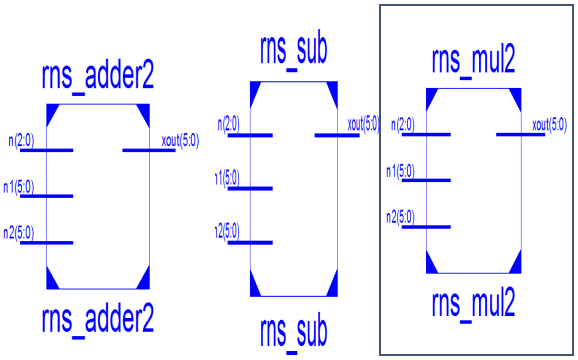

Figure 9: Top View of RNS Adder,subtractor and Multiplier

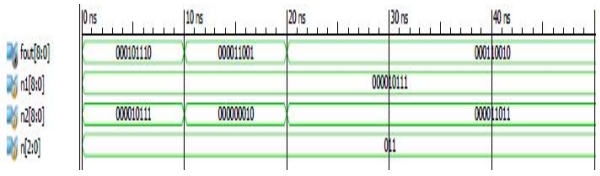

Figure 10: Timing Waveform of RNS based Adder Unit

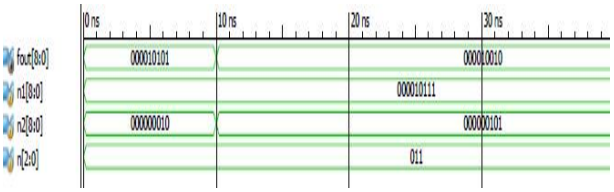

Figure 11: Timing Waveform of RNS based Subtractor Unit

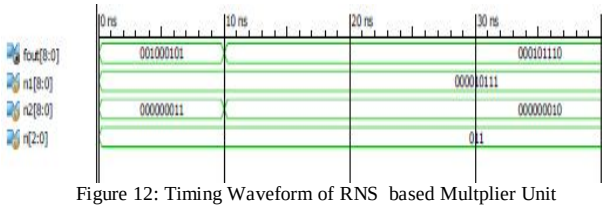

Figure 12: Timing Waveform of RNS based Multplier Unit

The Simulation of RNS based Addition, Subtraction and Multiplication Units are synthesized with the Device XC3S100E, package of CP132 and Family SPARTAN 3E and Corresponding Timing Waveforms are taken from the Test Bench as shown in Figure 10, 11 and 12.

Table I: RNS Based Adder,Subtractor And Multiplication Units for n=2

Topology for n=2	***No of slices***	***No of LUT's***	***Delay(ns)***
Addition	55	96	32.750
Subtraction	53	94	30.164
Multiplication	73	129	38.061

Table II. Rns Based Adder,Subtractor And Multiplication Units for n=3

Topology for n=3	***No of slices***	***No of LUT's***	***Delay(ns)***
Addition	107	188	37.355
Subtraction	108	190	37.148
Multiplication	113	201	40.388

From the above Table 1 &2 it shows that the RNS based Addition , Subtraction and Multiplication Unit for n=2 &3.

V. CONCLUSION

An Efficient RNS based Addition, Subtraction and Multiplication Units for moduli set $\{2^n\text{-}1, 2^n, 2^n\text{+}1\}$ for n=2 &3 has been implemented and simulated in Environment of xilinx ISE 13.2. From the result analysis it is observed that the proposed model is efficient when compared conventional adder,mltiplier and Subtraction Units.

VI. REFERENCES

[1] Wei Wang, M.N.S. Swamy, M.O. Ahmad and Yuke Wang,"The Applications of The New Chinese Remainder Theorems for Three Moduli Sets", Proceedings of IEEE Canadian Conference on Electrical and Computer Engineering Shaw Conference Center, Edmonton, Alberta, Canada May 9-12 1999.

[2] Bin Cao, Chip-Hong Chang and Thambipillai 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 Transactions On Circuits And Systems—I: Fundamental Theory And Applications, Vol. 50, No. 10, October 2003.

[3] Salvatore Pontraelli, Gian Carlo Cardarilli, Marco Re, Adelio Salsano, "Optimized implementation of RNS FIR filters based on FPGAs", Springer Journal of Signal Processing System, Vol.67, issue 3,pp.201-212, June 2012.

[4] A. Omondi and B. Premkumar, "Residue Number System: Theory and implementation", Imperial College Press, 2007, (ISBN 978-1-86094-866-4).

[5] Jean-Luc Beuchat, "Some Modular Adder and Multipliers for Field Programmable Gate Arrays", IEEE Proceedings of International Symposium on Parallel and Distributed Processing,v ol.17, pp.8 , April 2010.

[6] Somayeh Timarchi, Keivan Navi, "Improved Modulo 2n +1 Adder Design", World Academy of Science, Engineering and Technology, 2001

[7] Marco Re , Alberto Nannarelli , Gian Carlo Cardarilli , Roberto Lojacono, "FPGA realization of RNS to Binary signed conversion architecture", Proceedings of IEEE International Symposium on Circuits and Systems, Sydney, Australia, vol. 4, pp.350-353, May 2001

[8] S.Piestrak, "A high speed realization of a residue to binary number system Converter", IEEE Transactions on Circuits and systems-II, vol. 42, no. 10, October 1995.

[9] M. R. Schroeder, Number Theory in Science and Communication. Berlin, Germany: Springer-Verlag, 1984.

[10] A. P. Vinod and A. B. Premkumar, "A memoryless reverse converter for the 4-moduli superset $\{2^n\text{-}1 , 2^n , 2^n + 1, 2^{n+1}\text{-}1\}$" ,J. Circuits, Syst., Comput., vol. 10, no. 1&2, pp. 85–99, 2000.

[11] Somayyeh Jafarali Jassbi, Keivan Navi, and Ahmad khademzadeh, "An Optimum Moduli Set in Residue Number System", International Journal of Mathematical Forum,vol.5,pp. 2911-2918, March 2010.

[12] P. Samundiswary and S.kalpana, "Design and Analysis of RNS based FIR Filter using Verilog Language", International Journal of Computational Engineering and Management, vol.16, issue 6, November 2013.

[13] Chip-Hong Chang, Shibu Menon,Bin Cao and Thambipillai Srikanthan, "A Configurable Dual Mouli multi Operand Modular Adder", IEEE Symposium on Circuits and Systems pp.1168-1171,May 2005.

[14] R. Zimmerman, "Efficient VLSI implementation of modulo $(2^n \pm 1)$ addition and multiplication," in Proc. 14th IEEE Symp. Computer Arithmetic, pp. 158-167, Apr. 1999.