Journal of Computations & Modelling, vol.2, no.1, 2012, 93-108
ISSN: 1792-7625 (print), 1792-8850 (online)
International Scientific Press, 2012

Efficient Reverse Converter Design for Five Moduli Set $\left\{2^n, 2^{2n+1}-1, 2^{n/2}-1, 2^{n/2}+1, 2^n+1\right\}$

MohammadReza Taheri[1], Elham Khani[2], Mohammad Esmaeildoust[3] and Keivan Navi[3]

Abstract

In this paper, new design of reverse converter for the five moduli set $\left\{2^n, 2^{2n+1}-1, 2^{n/2}-1, 2^{n/2}+1, 2^n+1\right\}$ when n has even values is presented. The proposed reverse converter is designed in two levels architecture. In first level subset $\left\{2^n, 2^{2n+1}-1, 2^{n/2}-1, 2^{n/2}+1, 2^n+1\right\}$ is calculated by employing New Chinese Reminder Theorem-I (New CRT-I) and calculation of subset $\left\{(2^{2n+1}-1)(2^{2n}-1), 2^n\right\}$ in second level is based on Mixed Radix Conversion (MRC). The proposed reverse converter for the module set

[1] Microelectronic Laboratory of Shahid Beheshti University, GC, Tehran, Iran, e-mail: mrc-ecef@sbu.ac.ir
[2] Department of Computer Engineering, Science and Research Branch, Islamic Azad University, Tehran, Iran, e-mail: e.khani@srbiau.ac.ir
[3] Faculty of Electrical and Computer Engineering, Shahid Beheshti University, GC, Tehran, Iran, e-mail: {m_doust, navi}@sbu.ac.ir

Article Info: *Received* : December 25, 2011. *Revised* : January 30, 2012
Published online : April 20, 2012

$\left\{2^{n}, 2^{2n+1}-1, 2^{n/2}-1, 2^{n/2}+1, 2^{n}+1\right\}$ has achieved noticeable improvement in terms of speed compared to reverse converter previously presented for the modouli set $\left\{2^{2n+1}, 2^{n/2}-1, 2^{n/2}-1, 2^{n}+1, 2^{n}\right\}$ and other five moduli sets in literature.

Keywords: Residue number system, reverse converter, new Chinese reminder theorem-I, mixed radix conversion

1 Introduction

Arithmetic operation is one of the main parts of the digital systems. With growth of application, needs for speed up the arithmetic operation is sensible. Residue number system (RNS) has been considered as an alternative for binary system by researchers in past years. In residue number system, operation like addition, subtraction and multiplication can be replaced by parallel execution of small circuits [1]. Although RNS is not suitable for general purpose processors, its realization in special application such as image processing [2-3], digital signal processing [4], FIR filter [5-6] and cryptography [7-8] resulted in more speed and less power consumption over binary systems.

Binary to residue (forward) conversion, arithmetic operation and residue to binary (reverse) conversion are the three main parts of the RNS systems. RNS system is mainly consists of module set. The RNS module must be pair wise relatively prime. The dynamic range of an RNS system is defined in terms of the product of the module, and it denotes the interval of integers exclusively represented in RNS [1]. Efficiency of forward conversion, arithmetic operation and reverse conversion is related to careful selection of module set. Among these three parts, reverse converter has more complex architecture and its complexity will growth depend on the number of module. Therefore efficient design of reverse converter is needed in order to gain the benefit of the RNS.

Module set $\{2^n , 2^n - 1 , 2^n + 1\}$ [9] is the most famous module set but the provided dynamic ranges by this module set is not suitable for modern application. Therefore four module sets like $\{2^n , 2^n - 1 , 2^n + 1 , 2^{2n+1} + 1\}$ and $\{2^{2n} , 2^n - 1 , 2^n + 1 , 2^{2n} + 1\}$ [10] are reported. For more parallelism five module set $\{2^n , 2^n - 1 , 2^n + 1 , 2^{n+1} - 1 , 2^{n-1} + 1\}$ with arithmetic friendly module is reported in [11]. Inefficient multiplicative inverses are one of the main disadvantages of this module set. This leads to very complex hardware architecture of the reverse converter with large delay. In order to achieve fast and simple hardware implementation of reverse converter in five module RNS system and achieve tradeoff between arithmetic operation and reverse conversion, the module sets $\left\{2^n , 2^{n/2} - 1 , 2^{n/2} + 1 , 2^n + 1 , 2^{2n-1} - 1\right\}$ [12] and $\left\{2^n , 2^{n/2} - 1 , 2^{n/2} + 1 , 2^n + 1 , 2^{2n+1} - 1\right\}$ [13] are presented.

In this work different reverse converter architecture for the module set $\left\{2^n , 2^{n/2} - 1 , 2^{n/2} + 1 , 2^n + 1 , 2^{2n+1} - 1\right\}$ compared to [13] will be presented. The proposed reverse converter has achieved noticeable improvement in terms of delay of the reverse converter compared to [13].

This paper is organized as follows. The related RNS background is presented in section 2. The proposed architecture of the reverse converter is discussed in section 3. Section 4 presents the performance comparison of the proposed architecture with other five module reverse converters and finally section 5 concludes the paper.

2 RNS Background

RNS is represented by set of N integer number $\{P_1, P_2, ..., P_N\}$ that are pair wise relatively prime. The dynamic range (DR) is the product of the module and every integer number between 0 and (DR-1) can be uniquely represented as $X = (x_1, x_2, \ldots, x_N)$ where $x_i = X \bmod P_i$.

The addition, subtraction and multiplication operations on residues performed in parallel without carry propagation. Therefore large numbers can be presented by set of smaller numbers that and results in speed up the operation. Conversion of residue numbers to its equivalent in binary form could be achieved by Chinese Reminder Theorem (CRT), Mix Radix Conversion (MRC) and New CRT-I [1]. These theorems are described as follows:

By using Chinese Reminder Theorem equivalent of weighted binary number calculated from residue is as

$$X = \left| \sum_{i=1}^{N} \left| x_i L_i \right|_{P_i} M_i \right|_M \tag{1}$$

Where $M = P_1 \times P_2 \times \ldots \times P_N$, $M_i = M / P_i$ and $L_i = |M_i^{-1}|_{P_i}$ is the multiplicative inverse of M_i in modulus P_i. Mix Radix Conversion calculates equivalent of weighted binary number by

$$X = v_N \prod_{i=1}^{N-1} P_i + \ldots + v_3 P_2 P_1 + v_2 P_1 + v_1 \tag{2}$$

where

$$v_1 = x_1$$

$$v_2 = \left| (x_2 - v_1) \left| P_1^{-1} \right|_{P_2} \right|_{P_2}$$

$$v_3 = \left| ((x_3 - v_1) \left| P_1^{-1} \right|_{P_3} - v_2) \left| P_2^{-1} \right|_{P_3} \right|_{P_3}$$

In general

$$v_N = \left| (((x_N - v_1)\left|P_1^{-1}\right|_{P_N} - v_2)\left|P_2^{-1}\right|_{P_N} - \cdots - v_{N-1})\left|P_{N-1}^{-1}\right|_{P_N} \right|_{P_N}$$

$\left|P_i^{-1}\right|_{P_j}$ denotes the multiplicative inverse of P_i in modulus P_j.

New CRT-I computes the weighted number X as

$$X = x_1 + P_1 \left| \begin{array}{l} k_1(x_2 - x_1) + k_2 P_2 (x_3 - x_2) + \cdots \\ \quad + k_{N-1} P_2 P_3 \cdots P_{N-1}(x_N - x_{N-1}) \end{array} \right|_{P_2 P_3 \cdots P_N} \tag{3}$$

where

$$\left|k_1 \times P_1\right|_{P_2 P_3 \cdots P_N} = 1$$

$$\left|k_2 \times P_1 \times P_2\right|_{P_3 \cdots P_N} = 1$$

$$\left|k_{N-1} \times P_1 \times P_2 \times \cdots \times P_{N-1}\right|_{P_N} = 1$$

3 Reverse Converter Design

For efficient implementation of reverse converter for the module set

$$\left\{2^n , 2^{2n+1} - 1 , 2^{n/2} - 1 , 2^{n/2} + 1 , 2^n + 1\right\}$$

two levels design are employed. In first level subset

$$\left\{2^{2n+1} - 1 , 2^{n/2} - 1 , 2^{n/2} + 1 , 2^n + 1\right\}$$

are calculated by using New CRT-I. Second level stands for calculating the weighted number from the subset

$$\left\{(2^{2n+1} - 1)(2^{2n} - 1) , 2^n\right\}$$

based on MRC.

3.1 First level design

As mentioned before, first level calculate the weighted number from the subset

$$\left\{2^{2n+1}-1\ ,\ 2^{n/2}-1\ ,\ 2^{n/2}+1\ ,\ 2^{n}+1\right\}$$

and considering $P_1=2^{2n+1}-1$, $P_2=2^n+1$, $P_3=2^{n/2}+1$, $P_4=2^{n/2}-1$ by using New CRT-I. The required multiplicative inverses based on New CRT-I prescribed in Eq. (3) are as follows.

$$\left|K_1\times(2^{2n+1}-1)\right|_{2^{2n}-1}=1\rightarrow K_1=1 \tag{4}$$

$$\left|K_2\times(2^{2n+1}-1)(2^n+1)\right|_{2^n-1}=1\rightarrow K_2=2^{n-1} \tag{5}$$

$$\left|K_3\times(2^{2n+1}-1)(2^n+1)(2^{n/2}+1)\right|_{2^{n/2}-1}=1\rightarrow K_3=2^{n/2-2} \tag{6}$$

For the calculation of weighted number Z from its residues by using New CRT-I we have

$$Z=x_1+P_1\left|\begin{matrix}K_1\times(x_2-x_1)+K_2\times P_2\times(x_3-x_2)\\ +K_3\times P_2\times P_3(x_4-x_3)\end{matrix}\right|_{P_2\times P_3\times P_4} \tag{7}$$

By replacing the calculated multiplicative inverse in Eq. (7), results in

$$Z=x_1+(2^{2n+1}-1)\left|\begin{matrix}(x_2-x_1)+2^{n-1}\times(2^n+1)\times(x_3-x_2)+\\ 2^{n/2-2}\times(2^n+1)(2^{n/2}+1)(x_4-x_3)\end{matrix}\right|_{2^{2n}-1} \tag{8}$$

Eq. (8) can be rewritten as

$$Z=x_1+(2^{2n+1}-1)\left|z_3+z_1+z_2\right|_{2^{2n}-1} \tag{9}$$

where

$$z_1=\left|2^{n-1}\times(2^n+1)\times(x_3-x_2)\right|_{2^{2n}-1}$$

$$z_2=\left|2^{n/2-2}\times(2^n+1)(2^{n/2}+1)(x_4-x_3)\right|_{2^{2n}-1}$$

$$z_3=\left|(x_2-x_1)\right|_{2^{2n}-1}$$

Considering

$x_1 = x_{1,2n} \ldots x_{1,0}$, $x_2 = x_{2,n} \ldots x_{2,0}$, $x_3 = x_{3,n/2} \ldots x_{3,0}$ and $x_4 = x_{4,n/2-1} \ldots x_{4,0}$

for z_1 we have

$$z_1 = \left| 2^{n-1} \times (2^n + 1) \times (x_3 - x_2) \right|_{2^{2n}-1} \tag{10}$$

$$z_1 = \left| 2^{n-1} \times (2^n + 1) \times (\underbrace{0\ldots00}_{3n/2-1} x_{3,n/2} \ldots x_{3,0} - \underbrace{0\ldots00}_{n-1} x_{2,n} \ldots x_{2,0}) \right|_{2^{2n}-1} \tag{11}$$

$$z_1 = \left| 2^{n-1} \times (2^n + 1) \times (\underbrace{0\ldots00}_{3n/2-1} x_{3,n/2} \ldots x_{3,0} - \underbrace{0\ldots00}_{n-1} x_{2,n} \ldots x_{2,0}) \right|_{2^{2n}-1} \tag{12}$$

$$z_1 = \left| \begin{array}{l} x_{3,0} \underbrace{0\ldots00}_{n/2-1} x_{3,n/2} \ldots x_{3,0} \underbrace{0\ldots00}_{n/2-1} x_{3,n/2} \ldots x_{3,1} - \\ (x_{2,0} \underbrace{0\ldots00}_{n-1} x_{2,n} \ldots x_{2,1} + x_{2,n} \ldots x_{2,0} \underbrace{0\ldots00}_{n-1}) \end{array} \right|_{2^{2n}-1} \tag{13}$$

$$z_1 = \left| \begin{array}{l} x_{3,0} \underbrace{0\ldots00}_{n/2-1} x_{3,n/2} \ldots x_{3,0} \underbrace{0\ldots00}_{n/2-1} x_{3,n/2} \ldots x_{3,1} + \\ \overline{x}_{2,0} \underbrace{1\ldots11}_{n-1} \overline{x}_{2,n} \ldots \overline{x}_{2,1} + \overline{x}_{2,n} \ldots \overline{x}_{2,0} \underbrace{1\ldots11}_{n-1}) \end{array} \right|_{2^{2n}-1} \tag{14}$$

$$z_1 = \left| z_{11} + z_{12} + z_{13} \right|_{2^{2n}-1} \tag{15}$$

where

$$z_{11} = x_{3,0} \underbrace{0\ldots00}_{n/2-1} x_{3,n/2} \ldots x_{3,0} \underbrace{0\ldots00}_{n/2-1} x_{3,n/2} \ldots x_{3,1}$$

$$z_{21} = \overline{x}_{2,0} \underbrace{1\ldots11}_{n-1} \overline{x}_{2,n} \ldots \overline{x}_{2,1}$$

$$z_{31} = \overline{x}_{2,n} \ldots \overline{x}_{2,0} \underbrace{1\ldots11}_{n-1}$$

For z_2 we have

$$z_2 = \left| 2^{n/2-2} (2^n + 1)(2^{n/2} + 1)(\underbrace{0\ldots00}_{3n/2} x_{4,n/2-1} \ldots x_{4,0} - \underbrace{0\ldots00}_{3n/2-1} x_{3,n/2} \ldots x_{3,0}) \right|_{2^{2n}-1} \tag{16}$$

$$z_2 = \left| \begin{array}{l} 2^{n/2-2}(2^n+1)(\underbrace{0...00}_{n}x_{4,n/2-1}...x_{4,0}x_{4,n/2-1}...x_{4,0}) - \\ (\underbrace{0...00}_{n-1}x_{3,n/2}...x_{3,0}\underbrace{0...00}_{n/2} + \underbrace{0...00}_{3n/2-1}x_{3,n/2}...x_{3,0}) \end{array} \right|_{2^{2n}-1} \tag{17}$$

$$z_2 = \left| \begin{array}{c} 2^{n/2-2}(x_{4,n/2-1}...x_{4,0}x_{4,n/2-1}...x_{4,0}x_{4,n/2-1}...x_{4,0}x_{4,n/2-1}...x_{4,0} - \\ x_{3,n/2-1}...x_{3,0}\underbrace{0...00}_{n/2-1}x_{3,n/2}...x_{3,0}\underbrace{0...00}_{n/2-1}x_{3,\frac{n}{2}} - \\ \underbrace{0...00}_{n/2-1}x_{3,n/2}...x_{3,0}\underbrace{0...00}_{n/2-1}x_{3,n/2}...x_{3,0}) \end{array} \right|_{2^{2n}-1} \tag{18}$$

$$z_2 = \left| \begin{array}{c} x_{4,1}x_{4,0}x_{4,n/2-1}...x_{4,0}x_{4,n/2-1}...x_{4,0}x_{4,n/2-1}...x_{4,0}x_{4,n/2-1}...x_{4,2} + \\ \overline{x}_{3,1}\overline{x}_{3,0}\underbrace{1...1}_{n/2-1}\overline{x}_{3,n/2}...\overline{x}_{3,0}\underbrace{1...1}_{n/2-1}\overline{x}_{3,n/2}\overline{x}_{3,n/2-1}...\overline{x}_{3,2} + \\ 1\overline{x}_{3,n/2}...\overline{x}_{3,0}\underbrace{1...1}_{n/2-1}\overline{x}_{3,n/2}...\overline{x}_{3,0}\underbrace{1...1}_{n/2-2} \end{array} \right|_{2^{2n}-1} \tag{19}$$

For simplicity Eq. (19) can be rewritten as

$$z_2 = \left| z_{21} + z_{22} + z_{23} \right|_{2^{2n}-1} \tag{20}$$

where

$$z_{21} = x_{4,1}x_{4,0}x_{4,n/2-1}...x_{4,0}x_{4,n/2-1}...x_{4,0}x_{4,n/2-1}...x_{4,0}x_{4,n/2-1}...x_{4,2}$$

$$z_{22} = \overline{x}_{3,1}\overline{x}_{3,0}\underbrace{1...1}_{n/2-1}\overline{x}_{3,n/2}...\overline{x}_{3,0}\underbrace{1...1}_{n/2-1}\overline{x}_{3,n/2}\overline{x}_{3,n/2-1}...\overline{x}_{3,2}$$

$$z_{23} = 1\overline{x}_{3,n/2}...\overline{x}_{3,0}\underbrace{1...1}_{n/2-1}\overline{x}_{3,n/2}...\overline{x}_{3,0}\underbrace{1...1}_{n/2-2}$$

For z_3, we have

$$z_3 = \left| \underbrace{0...00}_{n-1}x_{2,n}...x_{2,0} - \underbrace{0...00}_{2n-1}x_{1,2n}...x_{1,0} \right|_{2^{2n}-1} \tag{21}$$

$$z_3 = \left| \underbrace{0...00}_{n-1}x_{2,n}...x_{2,0} + \underbrace{1...11}_{2n-1}\overline{x}_{1,2n} + \overline{x}_{1,2n-1}...\overline{x}_{1,0} \right|_{2^{2n}-1} \tag{22}$$

Therefore

$$z_3 = \left| z_{31} + z_{32} + z_{33} \right|_{2^{2n}-1} \tag{23}$$

where

$$z_{31} = \underbrace{0...00}_{n-1} x_{2,n} ... x_{2,0}$$

$$z_{32} = \underbrace{1...11}_{2n-1} \overline{x}_{1,2n}$$

$$z_{33} = \overline{x}_{1,2n-1} ... \overline{x}_{1,0}$$

After calculation of z_1, z_2 and z_3, Z in Eq. (9) can be considered as

$$Z = x_1 + (2^{2n+1} - 1) \times Y \tag{24}$$

where

$$Y = \left| z_{31} + z_{32} + z_{33} + z_{21} + z_{22} + z_{23} + z_{12} + z_{11} \right|_{2^{2n}-1}$$

Hardware implementation of Y is shown in Figure 1.

After calculation of Y, we have

$$Z = x_1 + (2^{2n+1} - 1) \times Y \tag{25}$$

By concatenation of x_1 with ($2n$+1) bit in binary form at the end of 2^{2n+1}Y, Eq.(25) can be rewritten as

$$Z = Y x_1 - Y \tag{26}$$

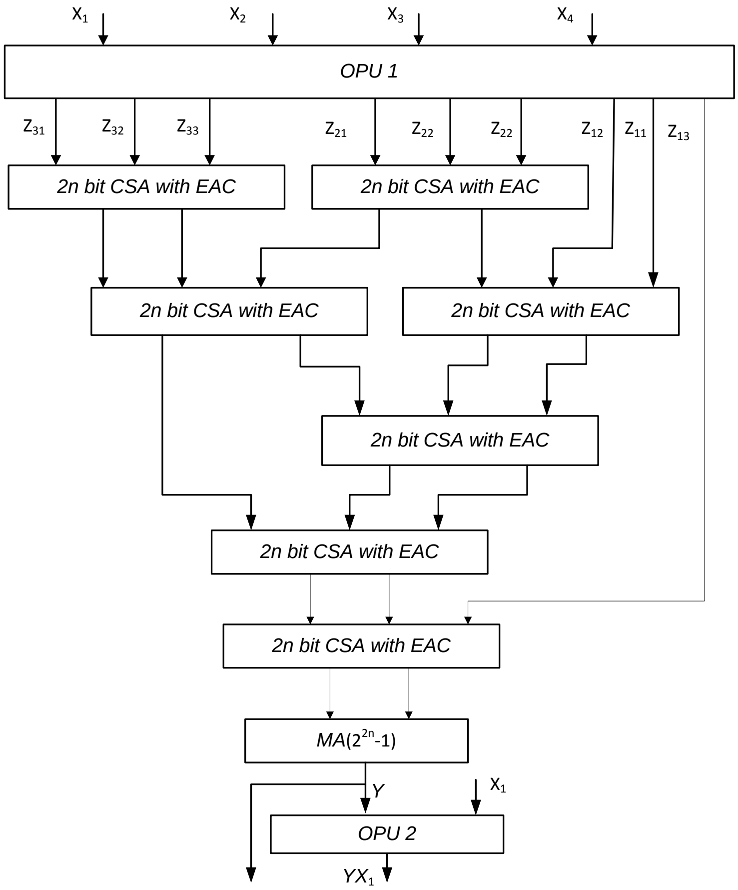

Figure 1: Hardware implementation of Z

3.2 Second level of the design

After calculation of *Z*, the subset $\{(2^{2n}-1)(2^{2n+1}-1), 2^n\}$ is achieved. In order to calculate the weighted number *X*, by using MRC and considering $P_{1234}=(2^{2n}-1)(2^{2n+1}-1)$ achieved from the previous level and $P_5 = 2^n$ we have

$$X = v_1 + v_2 P_{2345} \tag{27}$$

where

$$v_1 = Z$$

$$v_2 = \left|(x_5 - Z)\left|P_{1234}^{-1}\right|_{P_5}\right|_{P_5}$$

The required multiplicative inverse in Eq.(27) is recalculated as

$$\left|P_{1234}^{-1}\right|_{P_1} = \left|K \times (2^{2n} - 1)(2^{2n+1} - 1)\right|_{2^n} \rightarrow K = 1 \tag{28}$$

By replacing Eq.(26) and Eq.(27) in Eq.(28), we have

$$X = Yx_1 - Y + (2^{2n} - 1)(2^{2n+1} - 1)v_2 \tag{29}$$

where

$$v_2 = \left|x_5 - Z\right|_{2^n} \tag{30}$$

By replacing Eq.(26) in Eq.(30), we get

$$v_2 = \left|x_5 - Yx_1 + Y\right|_{2^n} \tag{31}$$

$$v_2 = \left|x_{5,n-1}\ldots x_{5,0} - x_{1,n-1}\ldots x_{1,0} + Y_{n-1}\ldots Y_0\right|_{2^n} \tag{32}$$

$$v_2 = \left|x_{5,n-1}\ldots x_{5,0} + k_1 + k_2 + 1\right|_{2^n} \tag{33}$$

where

$$k_1 = \bar{x}_{1,n-1}\ldots \bar{x}_{1,0}$$
$$k_2 = Y_{n-1}\ldots Y_0$$

Hardware Implementation of v_2 is shown in Figure 2.

By replacing v_2 in Eq.(29), we have

$$X = Yx_1 - Y + (2^{2n} - 1)(2^{2n+1} - 1)v_2 \tag{34}$$

$$X = v_2 Yx_1 - Y - v_2\underbrace{0\ldots00}_{2n} - v_2\underbrace{0\ldots00}_{2n+1} + v_2 \tag{35}$$

$$X = v_2 Yx_1 + (\bar{v}_2\bar{Y}) + \bar{v}_2\underbrace{1\ldots11}_{2n+1} + v_2 + 2 \tag{36}$$

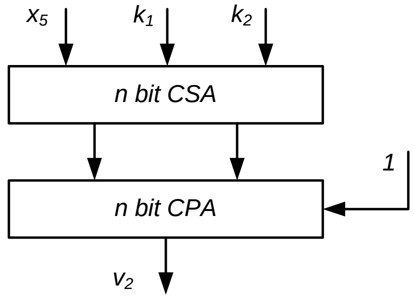

Figure 2: Hardware implementation of v_2

For reducing the number of levels of CSA in Eq.(36) in hardware implementation it can be rewritten as

$$X = v_2 Y x_1 + (\overline{v}_2 \overline{Y}) + \overline{v}_2 \underbrace{0...0}_{2n+1} + v_2 + 1 + 1\underbrace{0...0}_{2n+1}$$

$$X = h_1 + h_2 + h_3 + h_4$$

where

$$h_1 = v_2 Y x_1$$
$$h_2 = \overline{v}_2 \overline{Y}$$
$$h_3 = \overline{v}_2 \underbrace{0...0}_{n+1} v_2$$
$$h_4 = 1\underbrace{0...0}_{2n}1$$

Hardware implementation for calculation of X is shown in Figure 3.

4 Comparison

This section presents the comparison of the proposed reverse converter for the module set $\{2^{2n+1}-1, 2^n+1, 2^{n/2}-1, 2^{n/2}+1, 2^n\}$ with other five module set reverse converters reported in [11], [12] and [13]. As shown in Table 1, the proposed converter has $(10n+10)t_{FA}$, where t_{FA} denotes the delay of one bit full adder. The reverse converter proposed in [13] has the delay of $(12n+6)t_{FA}$. Therefore the proposed converter for the module set $\{2^{2n+1}-1,\ 2^n+1,\ 2^{n/2}-1,\ 2^{n/2}+1,\ 2^n\}$ with different levels of the design compared to [13] achieved in more speed in reverse conversion.

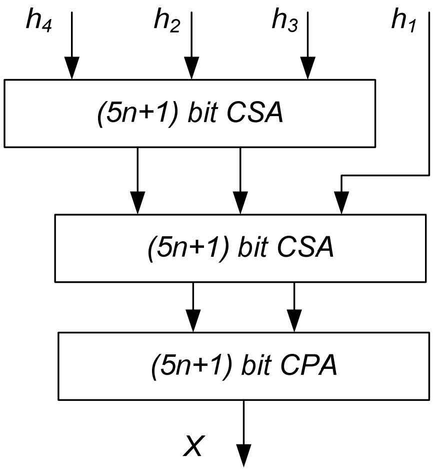

Figure 3: Hardware implementation of *X*

Table 1: Delay and area comparison of five moduli sets reverse converters

Converter	Hardware requirements	Unit gate area	Conversion delay	Unit gate delay
[11]	$((5n^2+43n+m^*)/6$ $+16n-1)A_{FA}$ $+(6n+1)A_{NOT}$	$(5n^2+43n+m^*)7/6$ $+118n-6$	$(18n+L^*+7)t_{FA}$	$72n+4L^*+28$
[12]	$(10n+5)A_{FA}+(7n-5)A_{XNOR}$ $+(7n-5)A_{OR}+(2n-3)A_{XOR}$ $+(2n-3)A_{AND}+(8n+2)A_{NOT}$	114n+5	$(13n+1)t_{FA}+3t_{NOT}$	52n+7
[13]	$(12.5n+6)A_{FA}$ $+(4.5n-1)A_{XNOR}$ $+(4.5n-1)A_{OR}$ $+(1.5n-1)A_{XOR}$ $+(1.5n-)A_{AND}+(7n+1)A_{NOT}$	112.5n+37	$(12n+6)t_{FA}+3t_{NOT}$	48n+27
Proposed	$(20n+n/2+2)A_{FA}$ $+(n-1)A_{XNOR}$ $+(n-1)A_{OR}+(2n+3)A_{XOR}$ $+(2n+3)A_{AND}+(9n/2)A_{NOT}$	149.5n+18	$(10n+9)t_{FA}$	40n+36

*m = n-4, 9n-12 and 5n-8 for n=6k-2,6k and 6k +2, respectively, and
L is the number of the levels of a CSA tree with ((n/2) +1) inputs.

Comparison with other five module sets are shown in Table 1. It can be seen that the proposed reverse converter for the module set $\{2^{2n+1}$-1, 2^n+1, $2^{n/2}$-1, $2^{n/2}$+1, $2^n\}$ has achieved to fastest implementation compared to other five module reverse converters.

In order to achieve fair comparison, unit gate delay and area are calculated which is shown in Table 1. In unit gate delay model, FA gates are considered with area of seven gates and delay of four gates. Each two input monotonic gates considered with one area and delay and XOR/XNOR gates are considered with two gates area and delay [12]. Unit gate delay comparison confirms faster design of the reverse converter for the module set $\{2^{2n+1}$-1, 2^n+1, $2^{n/2}$-1, $2^{n/2}$+1, $2^n\}$ is achieved.

5 Conclusion

In this paper, reverse converter with two levels design for the five module set $\left\{2^{n}\ ,\ 2^{2n+1}-1\ ,\ 2^{n/2}-1\ ,\ 2^{n/2}+1\ ,\ 2^{n}+1\right\}$ is presented. The proposed converter uses New CRT-I and MRC for first and second level, respectively. Noticeable improvement in speed of reverse conversion has achieved compared to other five module sets reverse converters.

References

[1] K. Navi, A.S. Molahosseini and M. Esmaeildoust, How to Teach Residue Number System to Computer Scientists and Engineers, *IEEE Transactions on Education*, **54**(1), (2011), 156-163.

[2] W. Wei, M.N.S. Swamy and M.O. Ahmad, RNS application for digital image processing, *Proceedings of the 4th IEEE international workshop on system-on-chip for real time applications*, (2004), 77-80.

[3] A. Ammar, A. Al Kabbany, M. Youssef and A. Emam, A secure image coding using residue number systems, *Procceding of the 18th National Radio Science Conference*, (2001), 399-405.

[4] G.C. Cardarilli, A. Nannarelli and M. Re, Residue Number System for Low-Power DSP Applications, *Procceding of 41nd IEEE Asilomar Conference on Signals, Systems, and Computers*, (2007), 1412-1416.

[5] R. Conway and J. Nelson, Improved RNS FIR Filter Architectures, *IEEE Transactions on Circuits and Systems-II*, **51**(1), (2004), 26-28.

[6] W.K. Jenkins and B.J. Leon, The use of residue number systems in the design of finite impulse response digital filters, *IEEE Transactions on Circuits and Systems*, **24**(4), (1977), 191-201.

[7] J.C. Bajard, L. Imbert, A Full RNS Implementation of RSA, *IEEE Transactions on Computers*, **53**(6), (2004), 769-774.

[8] D.M. Schinianakis, A. P. Fournaris, H. E. Michail, A. P. Kakarountas and T. Stouraitis, An RNS Implementation of an F_p Elliptic Curve Point Multiplier, *IEEE Transaction on Circuits and Systems I*, **56**(6), (2009), 1202-1213.

[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 Transactions on Signal Processing*, **50**(7), (2002), 1772-1779.

[10] 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 {2^n-1, 2^n+1, 2^{2n}, 2^{2n}+1} Based on New CRTs, *IEEE Transactions on Circuits and Systems-I*, **57**(4), (2010), 823-835.

[11] B. Cao, C.H. Chang and T. Srikanthan, A Residue-to-Binary Converter for a New Five-Moduli Set, *IEEE Transactions on Circuits and Systems-I*, **54**(5), (2007), 1041-1049.

[12] A.S. Molahosseini, C. Dadkhah, K. Navi, A New Five-Moduli Set for Efficient Hardware Implementation of the Reverse Converter, *IEICE Electronics Express*, **6**(14), (2009), 1006-1012.

[13] Mohammad Esmaeildoust, Keivan Navi and MohammadReza Taheri, High speed reverse converter for new five-moduli set $\{2^n, 2^{2n+1}-1, 2^{n/2}-1, 2^{n/2}+1, 2^n+1\}$, *IEICE Electron Express*, **7**(3), (2010), 118-125.