HIGH SPEED REVERSE CONVERTER FOR HIGH DYNAMIC RANGE MODULI SET

MohammadReza Taheri[1], Abdolreza Pirhoseinlo[2], Mojtaba Esmaeildoust[3], Mohammad Esmaeildoust[4], Keivan Navi[4]
[1] Microelectronic Laboratory of Shahid Beheshti University, GC, Tehran, Iran
[2] Department of Computer Engineering, Islamic Azad University, Arak, Iran
[3]Computer Engineering Department, Faculty of Engineering, University of Guilan, Iran
[4]Faculty of Electrical and Computer Engg., Shahid Beheshti University, GC, Tehran, Iran

ABSTRACT

In this paper a new reverse converter architecture for the five moduli set $\{2^n, 2^{n/2}-1, 2^{n/2}+1, 2^n+1, 2^{2n-1}-1\}$ is presented. The proposed converter is designed in two levels architecture by using of New Chinese Reminder Theorem-I (New CRT-I) and Mixed Radix Conversion (MRC). The proposed architecture has achieved significant improvement in terms of delay of the reverse converter compared to state-of-the-art reverse converters.

KEYWORDS: *Residue Number System, Digital Circuits, Residue Arithmetic, Reverse Converter*

I. INTRODUCTION

The residue number system is non-weighted number systems. Using this property has the advantages such as carry free operations, parallelism, fault tolerance and low power design in very large scale integration technology [1]. Speed up arithmetic operation in residue number system obtains by decomposing large binary operation into smaller residues. Therefore large number computations are replaced by smaller parallel operations. During the past decade, RNS has been widely used in the applications which requires intensive computation such image processing [2-3], Digital Signal Processing[4-6], and cryptography [7-9]. RNS based processors, unlike the binary systems,bear the extra cost of two components. These two components are the binary-to-residue (forward)and residue-to-binary (reverse) converters. Forward converter, converts thebinary number into its equivalent residues and reverse converter, converts the residues into their equivalent weighted number. Arithmetic unit is the core of RNS which performs arithmetic operations required by the application in parallel without carry propagation between residues digits. Reverse converter is a difficult process that affects the performance of the RNS. Form of the moduli set and number of moduli that chosen for RNS processor affects on dynamic range, speed and its VLSI implementation [10]. Different moduli set have been suggested for RNS. Most popular moduli set for past decade was $\{2^n, 2^n-1, 2^n+1\}$ where efficient reverse converter for this moduli set reported in [11]. For more parallelism four and five moduli sets are presented such as $\{2^n, 2^n-1, 2^n+1, 2^{2n+1}-1\}$, $\{2^{2n}, 2^n-1, 2^n+1, 2^{2n}+1\}$[12], $\{2^n, 2^n-1, 2^n+1, 2^{n+1}-1, 2^{n-1}-1\}$ [13], $\{2^n, 2^{n/2}-1, 2^{n/2}+1, 2^n+1, 2^{2n-1}-1\}$ [14] and $\{2^n, 2^{n/2}-1, 2^{n/2}+1, 2^n+1, 2^{2n+1}-1\}$ [15] are presented. Among the five moduli sets, moduli set $\{2^n, 2^n-1, 2^n+1, 2^{n+1}-1, 2^{n-1}-1\}$ enjoys well formed moduli with efficient arithmetic operation. The reverse converter for this moduli set has very high latency and hardware costbecause of inefficient multiplicative inverses. In order to achieve better trade-off between efficiency of arithmetic operation and reverse converter, other unbalanced moduli sets $\{2^n, 2^{n/2}-1, 2^{n/2}+1, 2^n+1, 2^{2n-1}-1\}$ [14] and $\{2^n, 2^{n/2}-1, 2^{n/2}+1, 2^n+1, 2^{2n+1}-1\}$

[15] with very simple hardware implementations of their reverse converter with higher speed compared to [13] are presented.
In this paper another design of reverse converter for the five moduli set $\{2^n, 2^{n/2}-1, 2^{n/2}+1, 2^n+1, 2^{2n-1}-1\}$ is presented. Two level designs are used in designing the proposed architecture by using New CRT-I and MRC for first and second level design, respectively. The proposed adder-based reverse converter has achieved faster implementation compared to other five moduli sets.
This paper is organized as follow, in section II the background of RNS is reviewed, in next section new reverse converter in two levels design for mentioned moduli set is proposed, in forth section hardware implementation of proposed reverse converter is represented and finally section V concludesthe paper.

II. PREVIOUS WORKS

Different moduli set have been proposed for RNS. Three moduli set $\{2^n, 2^n-1, 2^n+1\}$ was the most popular moduli set in the past decade which different reverse converters for this moduli set is reported in [16-20]. The best hardware implementation of the reverse converter for this moduli set is reported in [11]. In this report, three different design of residue to binary converters for the moduli set $\{2^n, 2^n-1, 2^n+1\}$ by using n-bit and $2n$-bit adders are presented. Converter which is based on $2n$-bit adder requires near half hardware area and better delay in comparison with previous works in this class of moduli set. The dynamic range of this moduli set is not qualified for applications which require larger dynamic range with more parallelism. Therefore another class of moduli set with more moduli or more dynamic range or both is reported in literatures. One of these approach is four moduli sets with $4n$-bit dynamic range like $\{2^n-3, 2^n+1, 2^n-1, 2^n+3\}$ [21], $\{2^n-1, 2^n, 2^n+1, 2^{n+1}-1\}$ and $\{2^n-1, 2^n, 2^n+1, 2^{n+1}+1\}$ [22], $\{2^n, 2^{n+1}-1, 2^n-1, 2^{n-1}-1\}$[23]. In [21], three different design of the reverse converters for the moduli set $\{2^n-3, 2^n+1, 2^n-1, 2^n+3\}$ are reported. The first design does not need any ROM and designed by adder base structure whereas others need ROM as well as combinational logic. In [22], two residue to binary converters for the two moduli set $\{2^n-1, 2^n, 2^n+1, 2^{n+1}-1\}$ and $\{2^n-1, 2^n, 2^n+1, 2^{n+1}+1\}$ are presented. The reverse converter of these moduli set are designed by MRC technique which apply on the two moduli set $\{\{2^n, 2^n-1, 2^n+1\}, 2^{n+1}-1\}$ and $\{\{2^n, 2^n-1, 2^n+1\}, 2^{n+1}-1\}$, respectively. The hardware cost is more economical than previous methods. Also residue to binary conversion delay also is reduced in this design. Efficient designs of residue to binary converter for the moduli set $\{2^n, 2^{n+1}-1, 2^n-1, 2^{n-1}-1\}$ is reported in [23]. This moduli set is completely free from modulo 2^k+1 type which results in high-speed modulo arithmetic. MRC algorithm is used to design residue to binary converter architectures. In [24], three moduli set $\{2^n, 2^{2n}-1, 2^{2n}+1\}$ with $5n$-bit dynamic range is presented. Chinese Remainder Theorem is used for design reverse converter for this moduli set. Simple hardware implementation by using only one CSA followed by a $4n$ bit modulo $2^{4n}-1$ adder, and a few gates, results in remarkable delay of reverse conversion. In [25], reverse converter for mosuli set $\{2^n-1, 2^n, 2^n+1, 2^{2n}+1\}$ with efficiency in delay conversion and hardware cost of its implementation with using CRT algorithm is presented. The disadvantage of these two moduli sets reported in [24-25] is use of modulo $2^{2n}+1$ which increase the latency of the RNS arithmetic unit. For overcome this problem moduli set $\{2^n-1, 2^n, 2^n+1, 2^{2n+1}-1\}$[12] is presented. In this work, New CRT-II is employed for designing an efficient reverse conversion. In class of five moduli with $5n$-bit dynamic range, moduli set such as $\{2^n, 2^n-1, 2^n+1, 2^n-2^{(n+1)/2}+1, 2^n+2^{(n+1)/2}+1\}$[26], $\{2^n, 2^n-1, 2^n+1, 2^{n+1}-1, 2^{n-1}-1\}$[13], $\{2^n, 2^{n/2}-1, 2^{n/2}+1, 2^n+1, 2^{2n-1}-1\}$ [14] and $\{2^n, 2^{n/2}-1, 2^{n/2}+1, 2^n+1, 2^{2n+1}-1\}$ [15] are presented. In [26] with using CRT, a full adder based reverse converter presented for the moduli set $\{2^n, 2^n-1, 2^n+1, 2^n-2^{(n+1)/2}+1, 2^n+2^{(n+1)/2}+1\}$. The problem of this moduli system is that the speed of the arithmetic unit of RNS is restricted to the low-performance modulo $2^n+2^{(n+1)/2}+1$. Cao et al. [13] proposed balanced and well-formed moduli set $\{2^n, 2^n-1, 2^n+1, 2^{n+1}-1, 2^{n-1}-1\}$ with efficient RNS arithmetic unit. In other hand the dynamic range of this moduli set are sufficient for today's necessity. The only disadvantage of this moduli set is its complex reverse converter due to inefficient forms of multiplicative inverse that lead to increasing the cost and the delay of reverse converter. Unbalanced moduli sets $\{2^n, 2^{n/2}-1, 2^{n/2}+1, 2^n+1, 2^{2n-1}-1\}$ and $\{2^n, 2^{n/2}-1, 2^{n/2}+1, 2^n+1, 2^{2n+1}-1\}$ with very simple hardware implementations of their reverse converter with higher speed compared to [13] and [26]. These moduli sets provides better trade-off between efficiency of arithmetic operation and reverse converter are presented.

III. RELATED BACKGROUND

Chinese Reminder Theorem (CRT)converts an RNS number into its equivalent weighted Number as follows:

$$X = \left| \sum_{i=1}^{n} \left| x_i N_i \right| P_i M_i \right|_M \tag{1}$$

Where

$$M = P_1 P_2 ... P_n$$

$$P_n, M_i = M / P_i$$

$$N_i = \left| M_i^{-1} \right| P_i$$

The CRT can be implemented in parallel channels followed by a modulus M adder.Modulo M reduction has very large latency and this can leads to inefficient hardware implementation of the reverse converter for high dynamic range moduli sets.
The weighted number *X* can be computed by New CRT-I as follows:

$$X = x_1 + P_1 \times \left| \begin{matrix} k_1 (x_2 - x_1) + k_2 P_2 (x_3 - x_2) + ... \\ + k_{n-1} P_2 P_3 ... P_{n-1} (x_n - x_{n-1}) \end{matrix} \right|_{P_2 P_3 ... P_n} \tag{2}$$

Where

$$\left| k_1 \times P_1 \right|_{P_2 P_3 ... P_n} = 1$$
$$\left| k_2 \times P_1 \times P_2 \right|_{P_3 ... P_n} = 1$$
$$\left| k_{n-1} \times P_1 \times P_2 \times ... \times P_{n-1} \right|_{P_n} = 1$$

Compared to CRT, the size of the final modulo reduction is reduced in New CRT-I. Mixed Radix Conversion (MRC) is another algorithm to convert the residues into the weighted number. To calculate *X*from its residues by MRC, we have

$$X = v_n \prod_{i=1}^{n-1} P_i + ... + v_3 P_2 P_1 + v_2 P_1 + v_1 \tag{3}$$

The coefficients v_is can be obtained from residues by

$$v_1 = x_1 \tag{4}$$

$$v_2 = \left| (x_2 - v_1) \left| P_1^{-1} \right|_{P_2} \right|_{P_2} \tag{5}$$

$$v_3 = \left| ((x_3 - v_1) \left| P_1^{-1} \right|_{P_3} - v_2) \left| P_2^{-1} \right|_{P_3} \right|_{P_3} \tag{6}$$

In the general case, we have

$$v_n = \left| (((x_n - v_1) \left| P_1^{-1} \right|_{P_n} - v_2) \left| P_2^{-1} \right|_{P_n} - \cdots - v_{n-1}) \left| P_{n-1}^{-1} \right|_{P_n} \right|_{P_n} \tag{7}$$

$\left| P_1^{-1} \right|_{Pj}$ indicates the multiplicative inverse of P_j modulus P_j.

IV. REVERSE CONVERTER DESIGN

In order to efficient design of reverse converter for the moduli set$\{2^n, 2^{n/2}-1, 2^{n/2}+1, 2^n+1, 2^{2n-1}-1\}$, two levels of design are employed. First level is designed by using New CRT-I and considering

subset$\{2^{n/2}-1,\ 2^{n/2}+1,\ 2^{n}+1,\ 2^{2n-1}-1\}$and in second level subset $\{(2^{n/2}-1)(\ 2^{2n-1}-1),\ 2^{n}\}$ is designed by using MRC.

3.1. First Level Design

In order to calculate the weighted number Z from its residues in subset $\{2^{n/2}-1,\ 2^{n/2}+1,\ 2^{n}+1,\ 2^{2n-1}-1\}$ by using New CRT-I, we have

$$Z = x_1 + P_1\left|k_1(x_2 - x_1) + k_2P_2(x_3 - x_2) + k_3P_2P_3(x_4 - x_3)\right|_{P_2P_3P_4} \tag{8}$$

By considering $P_1 = 2^{2n-1}-1,\ P_2 = 2^{n}+1,\ P_3 = 2^{n/2}+1, P_4 = 2^{n/2}-1$, we have

$$Z = x_1 + (2^{2n-1}-1)\left|\begin{matrix} k_1(x_2 - x_1) + k_2(2^{n}+1)(x_3 - x_2) + \\ k_3(2^{n}+1)(2^{n/2}+1)(x_4 - x_3) \end{matrix}\right|_{2^{2n}-1} \tag{9}$$

For the required multiplicative inverse in Eq. 9,we have

$$\left|k_1 \times (2^{2n-1}-1)\right|_{2^{2n}-1} = 1 \rightarrow k_1 = -2$$

$$\left|k_2 \times (2^{2n-1}-1)(2^{n}+1)\right|_{2^{n}-1} = 1 \rightarrow k_2 = -1$$

$$\left|k_3 \times (2^{2n-1}-1)(2^{n}+1)(2^{n/2}+1)\right|_{2^{n/2}-1} = 1 \rightarrow k_3 = -2^{\frac{n}{2}-1}$$

Eq. 9 can be rewritten as

$$Z = x_1 + (2^{2n-1}-1)Y \tag{10}$$

To calculate Y we have

$$Y = \left|\begin{matrix} (-2)(x_2 - x_1) + (-1)(2^{n}+1)(x_3 - x_2) + \\ (-2^{n/2-1})(2^{n}+1)(2^{n/2}+1)(x_4 - x_3) \end{matrix}\right|_{2^{2n}-1} \tag{11}$$

Eq. 11 can be rewrite as

$$Y = \left|Z_1 + Z_2 + Z_3\right|_{2^{2n}-1} \tag{12}$$

Where

$$Z_1 = \left|(-2)(x_2 - x_1)\right|_{2^{2n}-1}$$

$$Z_2 = \left|(-1)(2^{n}+1)(x_3 - x_2)\right|_{2^{2n}-1}$$

$$Z_3 = \left|(-2^{n/2-1})(2^{n}+1)(2^{n/2}+1)(x_4 - x_3)\right|_{2^{2n}-1}$$

By considering $x_1 = x_{1,2n-2}\ldots x_{1,0}$, $x_2 = x_{2,n}\ldots x_{2,0}$, $x_3 = x_{3,n/2}\ldots x_{3,0}$ and $x_4 = x_{4,n/2-1}\ldots x_{4,0}$, for Z_1 we have

$$Z_1 = \left|2\times(x_1 - x_2)\right|_{2^{2n}-1} \tag{13}$$

$$Z_1 = \left|2\times(x_{1,2n-2}\ldots x_{1,0} - x_{2,n}\ldots x_{2,0})\right|_{2^{2n}-1} \tag{14}$$

$$Z_1 = \left| 2\times \left(0x_{1,2n-2}\ldots x_{1,0} - \underbrace{0\cdots 00}_{(n-1)bit} x_{2,n}\ldots x_{2,0} \right) \right|_{2^{2n}-1} \tag{15}$$

$$Z_1 = \left| x_{1,2n-2}\ldots x_{1,0}0 + \underbrace{11\ldots 1}_{(n-2)bit}\bar{x}_{2,n}\ldots\bar{x}_{2,0}1 \right|_{2^{2n}-1} \tag{16}$$

$$Z_1 = \left| Z_{11} + Z_{12} \right|_{2^{2n}-1} \tag{17}$$

Where

$$Z_{11} = x_{1,2n-2}\ldots x_{1,0}0$$

$$Z_{12} = \underbrace{11\cdots 1}_{(n-2)bit}\bar{x}_{2,n}\ldots\bar{x}_{2,0}1$$

For Z_2 we have

$$Z_2 = \left| -(2^n+1)(x_3 - x_2) \right|_{2^{2n}-1} \tag{18}$$

$$Z_2 = \left| -\left(2^n+1\right)\left(\underbrace{00\cdots 0}_{\left(\frac{3}{2}n-1\right)bit} x_{3,n/2}\ldots x_{3,0} - \underbrace{00\cdots 0}_{(n-1)bit} x_{2,n}\ldots x_{2,0} \right) \right|_{2^{2n}-1} \tag{19}$$

$$Z_2 = \left| \begin{array}{l} x_{2,n-1}\ldots x_{2,0}\underbrace{00\cdots 0}_{(n-1)bit}x_{2,n} + \underbrace{00\cdots 0}_{(n-1)bit}x_{2,n}\ldots x_{2,0} - \\ \left(\underbrace{00\cdots 0}_{\left(n/2-1\right)bit} x_{3,n/2}\ldots x_{3,0}\underbrace{00\cdots 0}_{n\ bit} + \underbrace{00\cdots 0}_{\left(\frac{3}{2}n-1\right)bit} x_{3,n/2}\ldots x_{3,0} \right) \end{array} \right|_{2^{2n}-1} \tag{20}$$

$$Z_2 = \left| \begin{array}{l} x_{2,n-1}\ldots x_{2,0}\underbrace{00\cdots 0}_{(n-1)bit}x_{2,n} + \underbrace{00\cdots 0}_{(n-1)bit}x_{2,n}\ldots x_{2,0} + \\ \underbrace{11\cdots 1}_{\left(\frac{n}{2}-1\right)bit}\bar{x}_{3,n/2}\ldots\bar{x}_{3,0}\underbrace{11\cdots 1}_{\left(\frac{n}{2}-1\right)bit}\underbrace{\bar{x}_{3,n/2}\ldots\bar{x}_{3,0}}_{\left(\frac{n}{2}+1\right)bit} \end{array} \right|_{2^{2n}-1} \tag{21}$$

Therefore

$$Z_2 = \left| Z_{21} + Z_{22} + Z_{23} \right|_{2^{2n}-1} \tag{22}$$

Where

$$Z_{21} = \left| x_{2,n-1}\ldots x_{2,0}\underbrace{00\cdots 0}_{(n-1)bit}x_{2,n} \right|_{2^{2n}-1}$$

$$Z_{22} = \left| \underbrace{00\cdots 0}_{(n-1)bit} x_{2,n}\ldots x_{2,0} \right|_{2^{2n}-1}$$

$$Z_{23} = \left| \underbrace{11\cdots1}_{\left(\frac{n}{2}-1\right)bit} \bar{x}_{3,n/2} \ldots \bar{x}_{3,0} \underbrace{11\cdots1}_{\left(\frac{n}{2}-1\right)bit} \underbrace{\bar{x}_{3,n/2} \ldots \bar{x}_{3,0}}_{\left(\frac{n}{2}+1\right)bit} \right|_{2^{2n}-1}$$

For Z_3 we have

$$Z_3 = \left|(-2^{n/2-1})(2^n+1)(2^{n/2}+1)(x_4 - x_3)\right|_{2^{2n}-1} \tag{23}$$

$$Z_3 = \left|(-2^{n/2-1})(2^n+1)(2^{n/2}+1)\left(x_{4,n/2-1}\ldots x_{4,0} - x_{3,n/2}\ldots x_{3,0}\right)\right|_{2^{2n}-1} \tag{24}$$

$$Z_3 = \left| -2^{n/2-1} \times \left(\begin{array}{l} \left(2^n+1\right)\left(x_{4,n/2-1}\ldots x_{4,0} x_{4,n/2-1}\ldots x_{4,0}\right) - \\ \left(2^{\frac{n}{2}}+1\right)\left(\underbrace{00\cdots0}_{\left(\frac{n}{2}\text{-}1\right)bit} x_{3,n/2}\ldots x_{3,0} \underbrace{00\cdots0}_{\left(\frac{n}{2}\text{-}1\right)bit} x_{3,n/2}\ldots x_{3,0} \right) \end{array} \right) \right|_{2^{2n}-1} \tag{25}$$

$$Z_3 = \left| 2^{n/2-1} \times \left(\begin{array}{c} -x_4x_4x_4x_4 + x_{3,\frac{n}{2}-1}\ldots x_{3,0} \underbrace{00\cdots0}_{\left(\frac{n}{2}\text{-}1\right)bit} x_3 \underbrace{00\cdots0}_{\left(\frac{n}{2}\text{-}1\right)bit} x_{3,n/2} \\ + \underbrace{00\cdots0}_{\left(\frac{n}{2}\text{-}1\right)bit} x_{3,n/2}\ldots x_{3,0} \underbrace{00\cdots0}_{\left(\frac{n}{2}\text{-}1\right)bit} x_{3,n/2}\ldots x_{3,0} \end{array} \right) \right|_{2^{2n}-1} \tag{26}$$

$$Z_3 = \left| \begin{array}{c} \bar{x}_{4,0}\bar{x}_4\bar{x}_4\bar{x}_4\bar{x}_{4,\frac{n}{2}-1}\ldots\bar{x}_{4,1} + x_{3,0} \underbrace{00\cdots0}_{\left(\frac{n}{2}\text{-}1\right)bit} x_3 \underbrace{00\cdots0}_{\left(\frac{n}{2}\text{-}1\right)bit} x_{3,n/2}\ldots x_{3,1} \\ + x_{3,n/2}\ldots x_{3,0} \underbrace{00\cdots0}_{\left(\frac{n}{2}\text{-}1\right)bit} x_{3,n/2}\ldots x_{3,0} \underbrace{00\cdots0}_{\left(\frac{n}{2}\text{-}1\right)bit} \end{array} \right|_{2^{2n}-1} \tag{27}$$

$$Z_3 = \left| z_{31} + z_{32} + z_{33} \right|_{2^{2n}-1} \tag{28}$$

where

$$Z_{31} = \bar{x}_{4,0}\bar{x}_4\bar{x}_4\bar{x}_4\bar{x}_{4,\frac{n}{2}-1}\ldots\bar{x}_{4,1}$$

$$Z_{32} = x_{3,0} \underbrace{00\cdots0}_{\left(\frac{n}{2}\text{-}1\right)bit} x_3 \underbrace{00\cdots0}_{\left(\frac{n}{2}\text{-}1\right)bit} x_{3,n/2}\ldots x_{3,1}$$

$$Z_{33} = x_{3,n/2}\ldots x_{3,0} \underbrace{00\cdots0}_{\left(\frac{n}{2}\text{-}1\right)bit} x_{3,n/2}\ldots x_{3,0} \underbrace{00\cdots0}_{\left(\frac{n}{2}\text{-}1\right)bit}$$

Therefore *Y* can be calculated as

$$Y = \left| z_{11} + z_{12} + z_{21} + z_{22} + z_{23} + z_{31} + z_{32} + z_{33} \right|_{2^{2n}-1} \tag{29}$$

Hardware implementation ofEq. 29 is shown in figure 1. Bit organizer provides the required operands in Eq. 29. Carry Save Adders (CSA) with End Around Carry (EAC) are used to reduce the number of operands and then Modulo 2^{2n}–1 Adder (MA (2^{2n}–1)) is employed to calculate the *Y*.

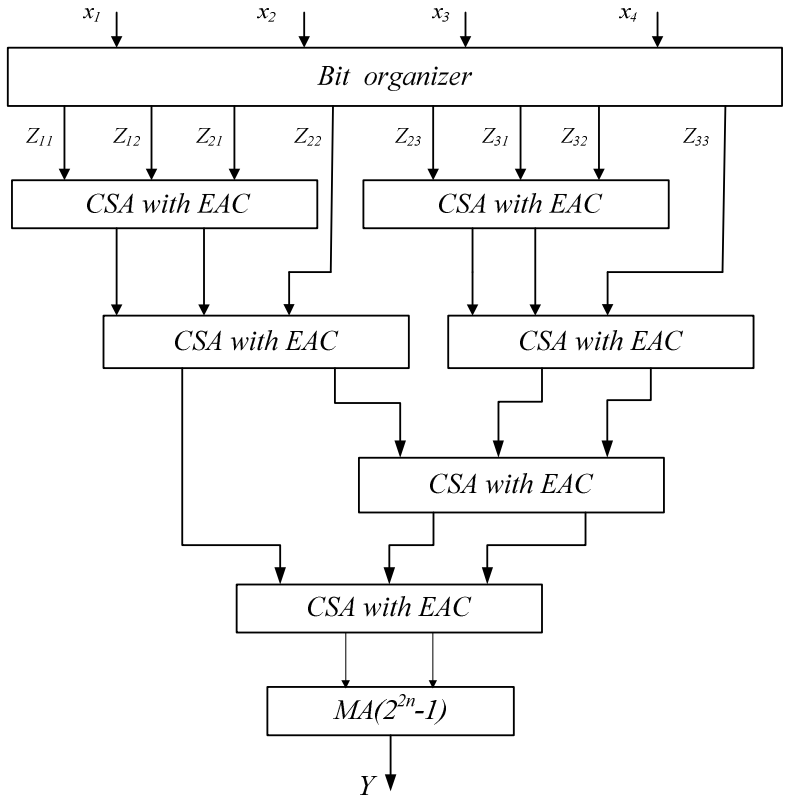


Figure 1. Hardware implementation of *Y*

After calculation of *Y*, to realize *Z* we have

$$Z = x_1 + (2^{2n-1} - 1)Y \tag{30}$$

$$Z = x_1 + Y\underbrace{00\cdots0}_{(2n-1)bit} - Y \tag{31}$$

$$Z = Y x_1 - Y \tag{32}$$

3.2. Second Level Design

Second level of the design consider the moduli set {(2^{2n}–1)(2^{2n-1}–1), 2^n} by using MRC. Considering P_{1234} = (2^{2n}–1)(2^{2n-1}–1) and using MRC we have

$$x = v_1 + v_2 p_{1234} \tag{33}$$

$$v_1 = Z \tag{34}$$

$$v_2 = \left| (x_5 - z) \left| P_{1234}^{-1} \right|_{2^n} \right|_{2^n} \tag{35}$$

For the required multiplicative inverses, we have

$$\left|P_{1234}^{-1}\right|_{2^n} \rightarrow \left|k(2^{2n}-1)(2^{2n-1}-1)\right|_{2^n} = 1$$

$$\left|P_{1234}^{-1}\right|_{2^n} = 1$$

Therefore

$$v_2 = \left|x_5 - Yx_1 + Y\right|_{2^n} \tag{36}$$

Eq. 36 can be rewritten as

$$v_2 = \left|x_{5,n-1}\ldots x_{5,0} - Y_{2n-1}\ldots Y_0 x_{1,2n-2}\ldots x_{1,0} + Y_{2n-1}\ldots Y_0\right|_{2^n} \tag{37}$$

$$v_2 = \left|x_{5,n-1}\ldots x_{5,0} - x_{1n-1}\ldots x_{1,0} + Y_{n-1}\ldots Y_0\right|_{2^n} \tag{38}$$

$$v_2 = \left|x_5 + v_{21} + v_{22} + 1\right|_{2^n} \tag{39}$$

Where

$$v_{21} = \bar{x}_{1,n-1}\ldots\bar{x}_{1,0}$$
$$v_{22} = Y_{n-1}\ldots Y_0$$

Therefore

$$X = v_1 + v_2(2^{2n}-1)(2^{2n-1}-1) \tag{40}$$

$$X = Yx_1 - Y + (v_2\underbrace{00\cdots0}_{2n\ bit} - v_2)(2^{2n-1}-1) \tag{41}$$

$$X = Yx_1 - Y + v_2\underbrace{00\cdots0}_{4n-1\ bit} - v_2\underbrace{00\cdots0}_{2n\ bit} - v_2\underbrace{00\cdots0}_{2n-1\ bit} + v_2 \tag{42}$$

$$X = v_2Yx_1 + \bar{v}_2\bar{Y} + \bar{v}_2 11\cdots1 + 2 + v_2 \tag{43}$$

$$X = v_2Yx_1 + \bar{v}_2\bar{Y} + \bar{v}_2 00\cdots0 + v_2 + 1 + 1\underbrace{00\cdots0}_{2n} \tag{44}$$

$$X = v_2Yx_1 + \bar{v}_2\bar{Y} + \bar{v}_2\underbrace{00\cdots0}_{(n-1)bit}v_2 + 1\ \underbrace{0\cdots0}_{(2n-1)bit}1 \tag{45}$$

$$K_1 = v_2Yx_1 \tag{46}$$

$$K_2 = \bar{v}_2\bar{Y} \tag{47}$$

$$K_3 = \bar{v}_2\underbrace{00\cdots0}_{(n-1)bit}v_2 \tag{48}$$

$$K_4 = 1\ \underbrace{0\cdots0}_{(2n-1)bit}1 \tag{49}$$

Therefore

$$X = K_1 + K_2 + K_3 + K_4 \tag{50}$$

Hardware implementation of X is shown in figure 2. First v_2 in Eq. 39 is implemented by using an n bit CSA followed by the Carry Propagate Adder (CPA). Then bit organizer in figure 2, provides the required shift and negation required in Eq. 46-49. In next step, two CSA followed by the CPA calculate the final result of X according to Eq. 50.

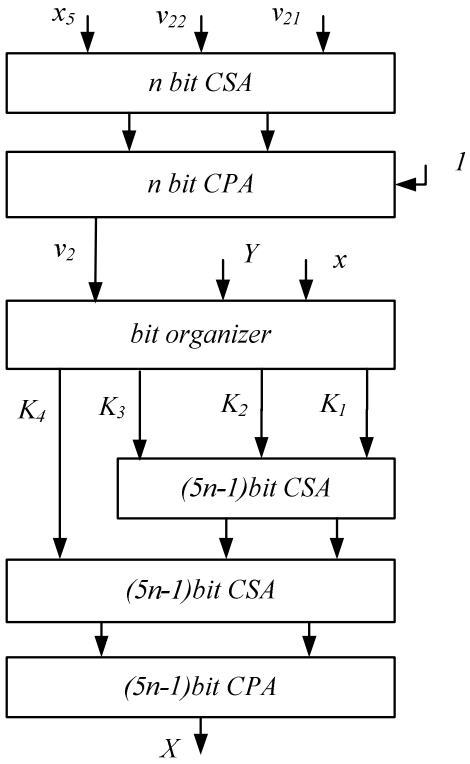


Figure 2. Hardware implementation of X

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

Converter	Hardware requirements	Conversion delay
[13]	$((5n^2+43n+m^*)/6+16n-1)A_{FA}+(6n+1)A_{NOT}$	$(18n+L^*+7)t_{FA}$
[14]	$(10n+5)A_{FA}+(7n-5)A_{XNOR}$ $+(7n-5)A_{OR}+(2n-3)A_{XOR}$ $+(2n-3)A_{AND}+(8n+2)A_{NOT}$	$(13n+1)t_{FA}+3t_{NOT}$
[15]	$(12.5n+6)A_{FA}+(4.5n-1)A_{XNOR}$ $+(4.5n-1)A_{OR}+(1.5n-1)A_{XOR}$ $+(1.5n-1)A_{AND}+(7n+1)A_{NOT}$	$(12n+6)t_{FA}+3t_{NOT}$
Proposed	$(17n+n/2+2)A_{FA}+(4n)A_{XNOR}$ $+(4n)A_{OR}+(8n-5)A_{XOR}$ $+(8n-5)A_{AND}+(7n/2)A_{NOT}$	$(10n+6)t_{FA}$

V. COMPARISON

Details of area and delay comparisons of the proposed reverse converter for the moduli set $\{2^{2n-1}-1, 2^n+1, 2^{n/2}-1, 2^{n/2}+1, 2^n\}$ with other five moduli sets reported in [13], [14] and [15] are shown in table 1. In order to achieve fair comparison, in calculations of delay and area, assumptions such as considered in [14-15] are employed. According to the obtained result in table 1, the proposed converter has $(10n+6)t_{FA}$, where t_{FA} denotes the delay of one bit full adder. The reverse converter

proposed in [13] has the delay of $(13n+1)t_{FA}$. Therefore the proposed converter for the moduli 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 [14] achieved in more speed in reverse conversion.Comparison with other five moduli sets are shown in table 1. It can be seen that the proposed reverse converter for the moduli set $\{2^{2n+1}-1, 2^n+1, 2^{n/2}-1, 2^{n/2}+1, 2^n\}$ has achieved fastest implementation compared to other five moduli reverse converters.

VI. CONCLUSION

We have presented a simple and efficient reverse converter architecture for the five moduli set $\{2^{2n+1}-1, 2^n+1, 2^{n/2}-1, 2^{n/2}+1, 2^n\}$. Two levels design, New CRT-I for subset $\{2^{n/2}-1, 2^{n/2}+1, 2^n+1, 2^{2n-1}-1\}$ and MRC for superset $\{(2^{2n}-1)(2^{2n-1}-1), 2^n\}$ are employed. Higher speed of the reverse converter has achieved compared to other five moduli set reverse converters in literature.

REFERENCES

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

[2]. W. Wei et al., (2004)"RNS application for digital image processing," Proceedings of the 4th IEEE international workshop on system-on-chip for real time applications. pp. 77 - 80.

[3]. A. Ammar, A. Al kabbany, M. Youssef, and A. Emam, (2001)"A secure image coding using residue number systems," Proc. of the 18th National Radio Science Conference.

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

[5]. R. Conway and J. Nelson, (2004) "Improved RNS FIR Filter Architectures," *IEEE Transactions on Circuits and Systems-II*, Vol. 51, No. 1, pp. 26-28.

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

[7]. J. C. Bajard, L. Imbert, (2004) "A Full RNS Implementation of RSA," *IEEE Transactions on Computers,* vol. 53, no. 6, pp. 769-774.

[8]. Marzie Gerami, Mohammad Esmaeildoust, Shirin Rezaei, Keivan Navi and Omid Hashemipour, (2011) "Four Moduli RNS Bases for Efficient Design of Modular Multiplication," Journal of Computations & Modelling, vol.1, no.2, 73-96.

[9]. D. M. Schinianakis, A. P. Fournaris, H. E. Michail, A. P. Kakarountas, andT. Stouraitis, (2009) "An RNS Implementation of an F_p Elliptic CurvePoint Multiplier", IEEE TRANSACTIONS ON CIRCUITS AND SYSTEMS—I, VOL. 56, NO. 6.

[10]. K. Navi, M. Esmaeildoust, and A. S. Molahosseini, (2011) "A General Reverse Converter Architecture with Low Complexity and High Performance," IEICE Transactions on Information and Systems, Vol. E94-D, No.2, pp. 264-273.

[11]. Y. Wang, X. Song, M. Aboulhamid and H. Shen, (2002) "Adder based residue to binary numbers converters for $(2^n-1, 2^n, 2^n+1)$,"*IEEE Transactions on Signal Processing*, vol. 50, no. 7, pp. 1772-1779.

[12]. A. S. Molahosseini, K. Navi, C. Dadkhah, O. Kavehei and S. Timarchi, (2010) " 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 Transaction on Circuit and System I, Vol. 57, No. 4, pp. 823-835.

[13]. B. Cao, C.H. Chang and T. Srikanthan, (2007) "A Residue-to-Binary Converter for a New Five-Moduli Set,"*IEEE Transactions on Circuits and Systems-I*, vol. 54, no. 5, pp.1041–1049.

[14]. A.S. Molahosseini, C. Dadkhah, K. Navi, (2009) "A New Five-Moduli Set for Efficient Hardware Implementation of the Reverse Converter," IEICE Electronics Express, vol. 6, no. 14, pp. 1006-1012.

[15]. Mohammad Esmaeildoust, Keivan Navi and MohammadReza Taheri, (2010) "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, Vol. 7, No. 3, pp.118-125.

[16]. D. Gallaher, F. Petry, and P. Srinivasan, (1997) "The digital parallel method for fast RNS to weighted number system conversion for specific moduli $\{2^n, 2^n-1, 2^n+1\}$," IEEE Trans. Circuits Syst. II, vol. 44, pp. 53–57.

[17]. S. Piestrak,(1995) "A high-speed realization of a residue to binary number system converter," IEEE Trans. Circuits Syst. II, vol. 42.

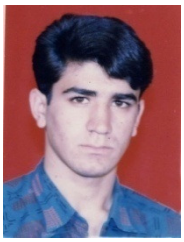
[18]. R. Conway and J. Nelson,(1999) "Fast converter for 3 moduli RNS using new property of CRT," IEEE Trans. Comput., vol. 48, pp. 852–860.

[19]. B. Vinnakota and V. V. B. Rao,(1994) "Fast conversion techniques for binary-residue number systems," IEEE Trans. Circuits Syst. I, vol. 41, pp. 927–929.

[20]. M. Bhardwaj, A. B. Premkumar, and T. Srikanthan, (1998) "Breaking the 2n-bit carry propagation barrier in residue to binary conversion for the $\{2^n, 2^n-1, 2^n+1\}$module set," IEEE Trans. Circuits Syst. II, vol. 45, pp. 998–1002.
[21]. P.V.A. Mohan,(2008) "New reverse converters for the moduli set $\{2^n-3, 2^n-1, 2^n+1, 2^n+3\}$," Elsevier Journal of Electronics and Communications (AEU), vol. 62, no. 9, pp. 643-658.
[22]. P. V. A. Mohan and A. B. Premkumar, (2007) "RNS-to-Binary Converters for Two Four-Moduli Set $\{2^n-1, 2^n, 2^n+1, 2^{n+1}-1\}$ and $\{2^n-1, 2^n, 2^n+1, 2^{n+1}+1\}$,"IEEE Transactions on Circuits and Systems-I, vol. 54, no. 6, pp. 1245-1254.
[23]. Mohammad Esmaeildoust, Keivan Navi, MohammadReza Taheri, Amir Sabbagh Molahosseini and Siavash Khodambashi, (2012) "Efficient RNS to binary converters for the new 4-moduli set $\{2^n, 2^{n+1}-1, 2^n-1, 2^{n-1}-1\}$", *IEICE Electron. Express*, Vol. 9, No. 1, pp.1-7.
[24]. Arash Hariri, Keivan Navi and Reza Rastegar, (2008)"A new high dynamic range moduli set with efficient reverse converter", International Journal of Computers and Mathematics with Applications, Elsevier, vol. 55 n.4, p.660-668.
[25]. B. Cao, C. H. Chang and T. Srikanthan, (2003) "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, vol. 50, no. 10, pp. 1296-1303.
[26]. A. A. Hiasat, (2005) "VLSI implementation of New Arithmetic Residue to Binary decoders," IEEE Transactions on VLSI Systems, vol. 13, no. 1, pp. 153-158.

Authors

Mohammadreza Taheri received B.Sc. degree in hardware engineering from Isfahan University, Iran, in 2007, and the M.Sc. degree at the Science and Research University branch of IAU, Tehran, Iran, in 2011 in computer system architecture. He is currently research assistance in Microelectronic Laboratory of Shahid Beheshti University, Tehran, Iran. His research interests include Cryptography, Computer Arithmetic with emphasis on Residue Number System and VLSI modeling and design of ultra-low power arithmetic circuits.



Abdolreza Pirhoseinlo was born in Tehran, Iran, in 1977. He received the B.Sc. degree from Islamic Azad University (IAU), Arak Branch (Arak, Iran) in 2002. He is M.Sc. student in Computer Architecture at IAU, Arak Branch. He is working on computer arithmetic especially on residue number system.

Mojtaba Esmaeildoust is B.Sc. student in hardware engineering in University of Guilan since 2009. His research interests include VLSI design, and public key cryptography with emphasis on elliptic curve cryptography.

Mohammad Esmaeildoust is Ph.D. candidate in Computer architecture at Shahid Beheshti University of Technology (Tehran, Iran). He received his M.Sc. degree in Computer architecture at Shahid Beheshti University of Technology (Tehran, Iran) in 2008. He received his B.Sc. degree in 2006 from shahed University in Hardware Engineering. His research interests include public key cryptography, reconfigurable computing, VLSI design, and computer arithmetic especially on residue number system.

Keivan Navi received the B.Sc. and M.Sc. degrees in computer hardware engineering from Beheshti University, Tehran, Iran, in 1987 and Sharif University of Technology, Tehran, Iran, in 1990, respectively. He also received the Ph.D. degree in computer architecture from Paris XI University, Paris, France, in 1995. He is currently Associate Professor in faculty of electrical and computer engineering of Beheshti University. His research interests include VLSI design, single electron transistors (SET), carbon nano tube, computer arithmetic, interconnection network and quantum computing. He has published over 70 ISI and research journal papers and over 70 IEEE, international and national conference paper.