

High speed reverse converter for new five-moduli set $\{2^n, 2^{2n+1}-1, 2^{n/2}-1, 2^{n/2}+1, 2^n+1\}$

Mohammad Esmaeildoust¹, Keivan Navi^{1a)},
and MohammadReza Taheri²

¹ Faculty of Electrical and Computer Engineering, Shahid Beheshti University GC, Tehran, Iran

² Department of Computer Engineering, Science and Research Branch, Islamic Azad University, Tehran, Iran

a) navi@sbu.ac.ir

Abstract: In this paper an efficient reverse converter for the new five moduli set $\{2^n, 2^{2n+1}-1, 2^{n/2}-1, 2^{n/2}+1, 2^n+1\}$ for even n is presented. With a little changes in latest introduced five moduli set $\{2^n, 2^{n/2}-1, 2^{n/2}+1, 2^n+1, 2^{2n-1}-1\}$ in order to achieve simple multiplicative inverse, this new moduli set is presented. The converter is designed in two levels architecture. The first level is based on CRT and the second one is based on MRC algorithm. The proposed converter achieved significant improvement in terms of speed with less hardware requirement comparing to other five moduli sets.

Keywords: reverse converter, computer arithmetic, residue number system

Classification: Integrated circuits

References

- [1] S. Timarchi and K. Navi, "Arithmetic circuits of redundant SUT-RNS," *IEEE Trans. Instrum. Meas.*, vol. 58, no. 9, pp. 2959–2968, 2009.
- [2] A. Omondi and B. Premkumar, *Residue Number Systems: Theory and Implementations*, Imperial College Press, London, 2007.
- [3] A. Hariri, K. Navi, and R. Rastegar, "A new high dynamic range moduli set with efficient reverse converter," *Computers and Mathematics with Applications*, vol. 55, no. 4, pp. 660–668, 2008.
- [4] A. S. Molahosseini, C. Dadkhah, K. Navi, and M. Eshghi, "Efficient MRC-Based Residue to Binary Converters for the New Moduli Sets $\{2^{2n}, 2^n-1, 2^{n+1}-1\}$ and $\{2^{2n}, 2^n-1, 2^{n-1}-1\}$," *IEICE Trans. Inf. & Syst.*, vol. E92-D, no. 9, pp. 1628–1638, Sept. 2009.
- [5] 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 Trans. Circuit Syst. I*, Accepted for publication, 2009.
- [6] B. Cao, C. H. Chang, and T. Srikanthan, "A Residue-to-Binary Converter for a New Five-Moduli Set," *IEEE Trans. Circuits Syst. I*, vol. 54, no. 5,

pp. 1041–1049, 2007.

- [7] A. S. Molahosseini, C. Dadkhah, and K. Navi, “A new five-moduli set for efficient hardware implementation of the reverse converter,” *IEICE Electron. Express*, vol. 6, no. 14, pp. 1006–1012, 2009.

1 Introduction

Residue Number System (RNS) is a carry free system. Using RNS leads to independent and fast arithmetic operations like addition, subtraction and multiplication. RNS is widely used in low power and high speed digital signal processing (DSP) [1, 2]. Designing efficient reverse converter is one of the important parts of the RNS. Efficiency of the reverse converter is depending on the form of the moduli. For many years the most popular moduli set was $\{2^n, 2^n - 1, 2^n + 1\}$. But nowadays the provided dynamic range by this moduli set is not sufficient for applications. Therefore moduli sets $\{2^n, 2^{2n} - 1, 2^{2n} + 1\}$ [3], $\{2^{2n}, 2^n - 1, 2^{n+1} - 1\}$ and $\{2^{2n}, 2^n - 1, 2^{n-1} - 1\}$ [4] with higher dynamic ranges are proposed by researchers. Furthermore to increase the parallelism of the RNS system, four moduli sets like $\{2^n - 1, 2^n, 2^n + 1, 2^{2n+1} - 1\}$ and $\{2^n - 1, 2^n + 1, 2^{2n}, 2^{2n} + 1\}$ are reported in [5]. To achieve more parallelism some five moduli set are reported like $\{2^n - 1, 2^n, 2^n + 1, 2^{n-1} - 1, 2^{n+1} - 1\}$ [6]. The mentioned moduli set is balanced but inefficient multiplicative inverse is one of the main disadvantages of this moduli set resulting in a time consuming process to execute reverse converter algorithm. In [7], authors reported a new five moduli set $\{2^n, 2^{n/2} - 1, 2^{n/2} + 1, 2^n + 1, 2^{2n-1} - 1\}$. In their approach, two-level design to achieve an efficient reverse converter are employed in which New Chinese Remainder Theorem (New CRT-I) and Mixed Radix Conversion (MRC) are used in level one and two, respectively.

In this paper a little changes in moduli set proposed in [7] are applied and moduli set $\{2^n, 2^{2n+1} - 1, 2^{n/2} - 1, 2^{n/2} + 1, 2^n + 1\}$ is yield to achieve a better multiplicative inverse. Two-level designs are employed that are completely different from the work reported in [7]. These two-levels consist of Chinese Remainder Theorem (CRT) and MRC. With this new design remarkable improvement in terms of speed of the reverse converter with less hardware requirement comparing to other mentioned five moduli sets is achieved.

2 Related Background

RNS systems includes N relatively prime integers (m_1, \dots, m_N) where $\gcd(m_i, m_j) = 1$ for $i, j = 1, \dots, N$ and $i \neq j$. Where $\gcd(a, b)$ demonstrate the greatest common divisor of “a” and “b”. An integer X is in range of $[0, M-1]$ where $M = m_1 \times \dots \times m_N$ is the dynamic range of the RNS system. Therefore we can represent each integer X uniquely like (x_1, x_2, \dots, x_N) where $x_i = |X|_{m_i} = (X \bmod m_i)$ implies that $0 < R_i < m_i - 1$. By CRT, the weighted number Z from its residues (x_1, x_2, \dots, x_N) can be achieved by the

following formula,

$$Z = \left(\sum_{i=1}^n \bar{m}_i \langle \bar{m}_i^{-1} \rangle_{m_i} \cdot x_i \right)_M \quad (1)$$

Where

$$M = \prod_{i=1}^N m_i, \quad \left| \bar{m}_i^{-1} \times \bar{m}_i \right| = 1, \quad \bar{m}_i = \frac{M}{m_i}$$

By MRC, the number X can be calculated from residues by

$$X = v_1 + v_2 m_1 + v_3 m_2 m_1 + \dots + v_n \prod_{i=1}^{n-1} m_i \quad (2)$$

The coefficients v_i s for three moduli can be obtained from residues by

$$\begin{aligned} v_1 &= x_1 \\ v_2 &= \left| (x_2 - x_1) \left| m_1^{-1} \right|_{m_2} \right|_{m_2} \\ v_3 &= \left| \left((x_3 - x_1) \left| m_1^{-1} \right|_{m_3} - v_2 \right) \left| m_2^{-1} \right|_{m_3} \right| \end{aligned}$$

3 Designing Reverse Converter

To achieve an efficient reverse converter for moduli set $\{2^n, 2^{2n+1}-1, 2^{n/2}-1, 2^{n/2}+1, 2^n+1\}$, two-level designs are employed. First, we consider $m_1 = 2^n$, $m_2 = 2^{2n+1}-1$, $m_3 = 2^{n/2}-1$, $m_4 = 2^{n/2}+1$, $m_5 = 2^n+1$ and $m_6 = 2^{2n}-1$. In first step the subset $\{2^{n/2}-1, 2^{n/2}+1, 2^n+1\}$ are calculated based on CRT and in second level, the set $\{2^n, 2^{2n+1}-1, 2^{2n}-1\}$ are calculated based on MRC, where m_6 is the multiplication of three moduli $\{2^{n/2}-1, 2^{n/2}+1, 2^n+1\}$.

3.1 Designing Converter for $\{2^{n/2}-1, 2^{n/2}+1, 2^n+1\}$ Based on CRT

The multiplicative inverses needed in CRT algorithm, are precalculated as follows:

$$\left| \bar{m}_3^{-1} \right|_{m_3} \rightarrow \left| k_1 \times (2^{n/2}+1)(2^n+1) \right|_{(2^{n/2}-1)} = 1 \rightarrow k_1 = 2^{(n-4)/2} \quad (3)$$

$$\left| \bar{m}_4^{-1} \right|_{m_4} \rightarrow \left| k_2 \times (2^{n/2}-1)(2^n+1) \right|_{(2^{n/2}+1)} \rightarrow k_2 = 2^{(n-4)/2} \quad (4)$$

$$\left| \bar{m}_5^{-1} \right|_{m_5} \rightarrow \left| k_3 \times (2^n-1) \right|_{(2^n+1)} = 1 \rightarrow k_3 = 2^{n-1} \quad (5)$$

The weighted number Z from its residues (x_3, x_4, x_5) , with considering $M_3 = 2^{n/2}-1$, $M_4 = 2^{n/2}+1$ and $M_5 = 2^n+1$ in CRT, can be calculated as follows

$$Z = \left| \begin{aligned} & (2^{n/2}+1)(2^n+1) \times 2^{(n-4)/2} \times x_3 \\ & + (2^{n/2}-1)(2^n+1) \times 2^{(n-4)/2} \times x_4 + (2^n-1) \times 2^{n-1} \times x_5 \end{aligned} \right|_{(2^{2n}-1)} \quad (6)$$

For residues in binary form we have: $x_1 = x_{1,n-1} \cdots x_{1,1}x_{1,0}$, $x_2 = x_{2,2n} \cdots x_{2,1}x_{2,0}$, $x_3 = x_{3,n-2/2} \cdots x_{3,1}x_{3,0}$, $x_4 = x_{4,n/2} \cdots x_{4,1}x_{4,0}$ and $x_5 = x_{5,n} \cdots x_{5,1}x_{5,0}$. We can rewrite equation (6) as

$$Z = |z_1 + z_2 + z_3|_{2^{2n-1}} \quad (7)$$

Where,

$$z_1 = \left| (2^{n/2} + 1)(2^n + 1) \times 2^{(n-4)/2} \times x_3 \right|_{2^{2n-1}} \quad (8)$$

$$z_2 = \left| (2^{n/2} - 1)(2^n + 1) \times 2^{(n-4)/2} \times x_4 \right|_{2^{2n-1}} \quad (9)$$

$$z_3 = \left| (2^n - 1) \times 2^{n-1} \times x_5 \right|_{2^{2n-1}} \quad (10)$$

In the equations $\{, \}$ denotes the concatenation.

In binary form we have,

$$z_1 = \left| 2^{(n-4)/2} \times (2^n + 1)(2^{n/2} + 1) \times (x_{3,n-2/2}) \cdots x_{3,1}x_{3,0} \right|_{2^{2n-1}} \quad (11)$$

$$\begin{aligned} z_1 &= \left| 2^{(n-4)/2} \left(\underbrace{x_{3,n-2/2} \cdots x_{3,0}}_{n \text{ bit}} \underbrace{x_{3,n-2/2} \cdots x_{3,0}}_{n \text{ bit}} \right) \right|_{2^{2n-1}} \\ &= x_{3,1}x_{3,0} \underbrace{x_{n-2/2} \cdots x_0}_{n/2 \text{ bit}} \underbrace{x_{n-2/2} \cdots x_0}_{n/2 \text{ bit}} \underbrace{x_{n-2/2} \cdots x_0}_{n/2 \text{ bit}} x_{3,n-2/2} \cdots x_{3,3}x_{3,2} \end{aligned} \quad (12)$$

$$z_2 = \left| (2^{n/2} - 1)(2^n + 1) \times 2^{(n-4)/2} \times \left(\underbrace{0 \cdots 00}_{(n-2)/2 \text{ bit}} \underbrace{x_{4,n/2} \cdots x_{4,1}x_{4,0}}_{(n+2)/2 \text{ bit}} \right) \right|_{2^{2n-1}} \quad (13)$$

$$k_1 = \underbrace{0 \cdots 00}_{(n-2)/2 \text{ bit}} \underbrace{x_{4,n/2} \cdots x_{4,1}x_{4,0}}_{(n+2)/2 \text{ bit}} \quad (14)$$

$$z_2 = \left| 2^{(n-4)/2} \times (2^{n/2} - 1) \times (k_1, k_1) \right|_{2^{2n-1}} \quad (15)$$

$$z_2 = \left| 2^{(n-4)/2} \times \left(\underbrace{x_{4,(n-2)/2} \cdots x_{4,1}x_{4,0}}_{n/2 \text{ bit}} k_1 \underbrace{0 \cdots 00}_{(n-2)/2 \text{ bit}} x_{4,n/2} - k_1, k_1 \right) \right|_{2^{2n-1}} \quad (16)$$

$$z_2 = \left| \begin{array}{c} x_{4,1}x_{4,0}k_1 \underbrace{0 \cdots 00}_{(n-2)/2 \text{ bit}} \underbrace{x_{4,n/2} \cdots x_{4,2}}_{(n-2)/2} \\ + 1\bar{x}_{4,n/2} \cdots \bar{x}_{4,2}\bar{x}_{4,1}\bar{x}_{4,0}\bar{k}_1 \underbrace{1 \cdots 11}_{(n-4)/2} \end{array} \right|_{2^{2n-1}} \quad (17)$$

$$z_2 = |z_{21} + z_{22}|_{2^{2n-1}} \quad (18)$$

$$\begin{aligned} z_{21} &= x_{4,1}x_{4,0}k_1 \underbrace{0 \cdots 00}_{(n-2)/2 \text{ bit}} \underbrace{x_{4,n/2} \cdots x_{4,2}}_{(n-2)/2} \\ z_{22} &= 1\bar{x}_{4,1}\bar{x}_{4,0}\bar{k}_1\bar{x}_{4,n/2} \cdots \bar{x}_{4,2} \underbrace{1 \cdots 11}_{(n-4)/2} \end{aligned} \quad (19)$$

$$z_3 = \left| (2^n - 1) \times 2^{n-1} \times (x_{5,n} \cdots x_{5,1}x_{5,0}) \right|_{2^{2n-1}} \quad (20)$$

$$z_3 = \left| 2^{n-1} \left(x_{5,n-1} \cdots x_{5,1}x_{5,0} \underbrace{0 \cdots 00}_{n-1 \text{ bit}} x_{5,n} + \underbrace{1 \cdots 11}_{n-1 \text{ bit}} \bar{x}_{5,n} \cdots \bar{x}_{5,1}\bar{x}_{5,0} \right) \right|_{2^{2n-1}} \quad (21)$$

$$z_3 = \left| \left(x_{5,0} \underbrace{0 \cdots 00}_{n-1 \text{ bit}} x_{5,n} \cdots x_{5,1} + \bar{x}_{5,n} \cdots \bar{x}_{5,1}\bar{x}_{5,0} \underbrace{1 \cdots 11}_{n-1 \text{ bit}} \right) \right|_{2^{2n-1}} \quad (22)$$

$$z_3 = |z_{31} + z_{32}|_{2^{2n-1}} \quad (23)$$

$$z_{31} = x_{5,0} \underbrace{0 \cdots 00}_{n-1 \text{ bit}} x_{5,n} \cdots x_{5,1} \quad \text{and} \quad z_{32} = \bar{x}_{5,n} \cdots \bar{x}_{5,1}\bar{x}_{5,0} \underbrace{1 \cdots 11}_{n-1 \text{ bit}} \quad (24)$$

3.2 Designing the Converter for $\{2^n, 2^{2n+1} - 1, 2^{2n} - 1\}$ Based on MRC

With using MRC algorithm mentioned in equation (2) for these moduli set we have: $X = x_1 + 2^n(v_2 + v_3 \times (2^{2n+1} - 1))$. Therefore we can consider $X = x_1 + 2^nY$, where $Y = v_2 + v_3 \times (2^{2n+1} - 1)$. Since x_1 has n bits, with calculating Y and concatenating x_1 at the end of Y , weighted number X can be achieved from its residues. Based on MRC algorithm, the multiplicative inverses can be calculated as below

$$\left| \left| m_1^{-1} \right|_{m_2} \times 2^n \right|_{2^{2n+1}-1} = 1 \rightarrow \left| m_1^{-1} \right|_{m_2} = 2^{n+1} \quad (25)$$

$$\left| \left| m_1^{-1} \right|_{m_6} \times 2^n \right|_{2^{2n}-1} = 1 \rightarrow \left| m_1^{-1} \right|_{m_6} = 2^n \quad (26)$$

$$\left| \left| m_2^{-1} \right|_{m_6} \times (2^{2n+1} - 1) \right|_{2^{2n}-1} = 1 \rightarrow \left| m_2^{-1} \right|_{m_6} = 1 \quad (27)$$

With considering $Z = z_{2n-1} \cdots z_1 z_0$ as $2n$ bit in modulo $2^{2n} - 1$, we have

$$v_2 = \left| (x_2 - x_1) \times 2^{n+1} \right|_{2^{2n+1}-1} \quad (28)$$

$$v_2 = \left| x_{2,n-1} \cdots x_{2,0}x_{2,2n} \cdots x_{2,n} + \bar{x}_{1,n-1} \cdots \bar{x}_{1,0} \underbrace{1 \cdots 11}_{n+1 \text{ bit}} \right|_{2^{2n+1}-1} \quad (29)$$

Where,

$$v_{21} = x_{2,n-1} \cdots x_{2,0} x_{2,2n} \cdots x_{2,n} \quad \text{and} \quad v_{22} = \bar{x}_{1,n-1} \cdots \bar{x}_{1,0} \underbrace{1 \cdots 11}_{n+1 \text{ bit}} \quad (30)$$

$$v_3 = \left| \left(z_{2n-1} \cdots z_0 - \underbrace{0 \cdots 00}_{n \text{ bit}} x_{1,n-1} \cdots x_{1,0} \right) \times 2^n - v_2 \right|_{2^{2n-1}} \quad (31)$$

$$v_3 = \left| \begin{aligned} & z_{n-1} \cdots z_0 z_{2n-1} \cdots z_{n-2} + \bar{x}_{1,n-1} \cdots \bar{x}_{1,0} \underbrace{1 \cdots 11}_{n \text{ bit}} \\ & + \underbrace{1 \cdots 11}_{2n-1 \text{ bit}} \bar{v}_{2,2n} \cdots \bar{v}_{2,0} \end{aligned} \right|_{2^{2n-1}} \quad (32)$$

$$v_3 = |v_{31} + v_{32} + v_{33} + v_{34}|_{2^{2n-1}} \quad (33)$$

Where

$$\begin{aligned} v_{31} &= z_{n-1} \cdots z_0 z_{2n-1} \cdots z_{n-2}, \quad v_{32} = \bar{x}_{1,n-1} \cdots \bar{x}_{1,0} \underbrace{1 \cdots 11}_{n \text{ bit}} \\ v_{33} &= \underbrace{1 \cdots 11}_{2n-1 \text{ bit}} \bar{v}_{2,2n} \quad \text{and} \quad v_{34} = \bar{v}_{2,2n-1} \cdots \bar{v}_{2,0} \end{aligned} \quad (34)$$

After calculating v_2 and v_3 , we have:

$$Y = v_{2,2n} \cdots v_{2,0} + (v_{3,2n-1} \cdots v_{3,0})(2^{2n+1} - 1) \quad (35)$$

$$Y = v_{2,2n} \cdots v_{2,0} + v_{3,2n-1} \cdots v_{3,0} \underbrace{0 \cdots 00}_{2n+1 \text{ bit}} - v_{3,2n-1} \cdots v_{3,0} \quad (36)$$

$$Y = k - v_{3,2n-1} \cdots v_{3,0} \quad (37)$$

$$k = v_{3,2n-1} \cdots v_{3,0} v_{2,2n} \cdots v_{2,0} \quad (38)$$

4 Hardware Implementation

Hardware implementation of the proposed reverse converter is shown in Figure 1. Designing the first level is based on the equations (12), (18), (23) and (29). For designing the first level, modulo $(2^{2n} - 1)$ adder is needed. To achieve this, CSA with EAC tree are used to create the inputs of the modulo $(2^{2n} - 1)$ adders. The result of modulo $(2^{2n} - 1)$ adder is Z . Calculating v_2 in second level is independent from the result of Z . Therefore in the first level, modulo $(2^{2n+1} - 1)$ adder is used to calculate v_2 . So, more parallelism and speed is achieved. Designing the second level is based on the equations (33) and (37). Two stages CSA with EAC are employed to create the input of modulo $(2^{2n} - 1)$ adder. After that, $(4n + 1)$ bits regular CPA with '1' carry in, is used to achieve Y . Finally with concatenating x_1 as n bits at the LSB of Y , weighted number X will be achieved from its residues.

5 Performance Evaluation

Comparison results regarding to speed and area of the reverse converters are done between the proposed moduli set $\{2^n, 2^{2n+1} - 1, 2^{n/2} - 1, 2^{n/2} + 1, 2^n + 1\}$ and the moduli sets $\{2^n - 1, 2^n, 2^n + 1, 2^{n-1} - 1, 2^{n+1} - 1\}$ [6] and $\{2^n, 2^{n/2} - 1, 2^{n/2} + 1, 2^n + 1, 2^{2n-1} - 1\}$ [7]. Dynamic range of the proposed moduli set is higher than the other mentioned moduli sets. The converters proposed in [6] and [7] have $(18n + L + 2)t_{FA}$ and $(13n + 1)t_{FA} + 3t_{NOT}$ delay, respectively. The proposed converter has $(12n + 6)t_{FA} + 3t_{NOT}$ delay for its reverse converter. Therefore the proposed converter is faster than the other reverse converters. Unit gate delay in order to achieve a fair comparison is shown in Table I. In this 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 [7]. Results of Table I confirm that remarkable improvement for speed of reverse converter and degraded hardware requirement are achieved comparing to other five moduli sets.

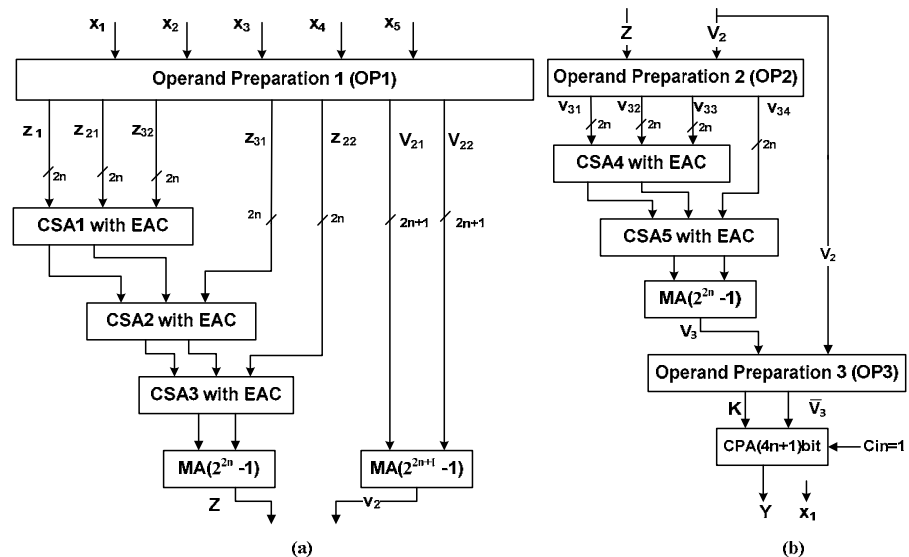


Fig. 1. Hardware architecture: (a) First level, (b) Second level

Table I. Performance Comparison for different five moduli sets

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

* $m=n-4, 9n-12$ 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.

6 Conclusion

This paper introduces a new five moduli set $\{2^n, 2^{2n+1} - 1, 2^{n/2} - 1, 2^{n/2} + 1, 2^n + 1\}$ with efficient implementation for its reverse converter. The design of the reverse converter has been realized in two-level architecture. The mixed of CRT and MRC algorithms constituted these two levels. Comparison with other latest five moduli sets shows that we have achieved a significant improvement in terms of speed and area in reverse converter implementation.