ELectronics EXpress

IEICE Electronics Express, Vol.9, No.1, 8–15

Reverse converter for the flexible moduli set $\{2^{n+k}, 2^{2n-1}-1, 2^{n/2}+1, 2^{n/2}-1\}$

Mohammad Reza Noorimehr[1a)], **Mehdi Hosseinzadeh**[1], **and Reza Farshidi**[2]

[1] *Science and Research Branch, Islamic Azad University, Tehran, Iran*

[2] *Department of Computer Engineering, Dezful Branch, Islamic Azad University, Dezful, Iran*

a) *R.noorimehr@srbiau.ac.ir*

Abstract: The speed of reverse converters in Residue Number System is one the most important and effective factors which is strictly dependent on the selected moduli set. In this paper, the four-moduli set $\{2^{n+k}, 2^{2n-1}-1, 2^{n/2}+1, 2^{n/2}-1\}$ is introduced with flexible dynamic range 4n to 5n where n is even and k < n. Then a high-speed two-level architecture reverse converter is designed for it based on mix-radix conversion (MRC) algorithm. A comparison to the similar recently introduced moduli sets $\{2^{n/2}-1, 2^{n/2}+1, 2^n+1, 2^{2n+1}-1\}$ and $\{2^{2n}, 2^{2n+1}-1, 2^{n/2}+1, 2^{n/2}-1\}$ shows that the proposed reverse converter has more conversion speed.

Keywords: reverse converter, residue arithmetic, VLSI architecture

Classification: Integrated circuits

References

[1] A. Omondi and B. Premkumar, *Residue Number Systems: Theory and Impleme- ntations*, Imperial College Press, London, 2007.

[2] K. Navi, A. S. Molahosseini, and M. Esmaeildoust, "How to Teach Residue Number System to Computer Scientists and Engineers," *IEEE Trans. Educ.*, vol. 54, p. 156, Feb. 2011.

[3] A. S. Molahosseini, F. Teymouri, and K. Navi, "A New Four - Modulus RNS to Binary Converter," *Proc. IEEE International Symposium on Circuits and Systems (ISCAS'10)*, 2010.

[4] M. R. Noorimehr, M. Hosseinzadeh, and R. Farshidi, "A new four-moduli set with high speed RNS arithmetic unit and efficient reverse converter," *IEICE Electron. Express*, vol. 7, no. 20, pp. 1584–1591, 2010.

[5] S. J. Piestrak, "Design of residue generators and multioperand modular adders using carry-save adders," *IEEE Trans. Comput.*, vol. 423, no. 1, pp. 68–77, Jan. 1994.

[6] 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.

DOI: 10.1587/elex.9.8
Received September 30, 2011
Accepted December 02, 2011
Published January 10, 2012

1 Introduction

Residue Number System (RNS) offers high- speed arithmetic because there is no carry propagation between modulus. Hence, this numeric system can be used in applications require high performance arithmetic such as Digital Signal processing [1]. One of the most important factors that determine the performance of an RNS system is the delay of its reverse converter because the more conversion delay may counteract the speed of arithmetic unit [2]. The speed of the reverse converter as well as the speed and complexity of the arithmetic unit are strictly dependent upon the selected moduli set. Many moduli sets have been introduced until now. Among them, the recently introduced four-moduli sets $\{2^{n/2}-1, 2^{n/2}+1, 2^n+1, 2^{2n+1}-1\}$ [3] and $\{2^{2n}, 2^{2n+1}-1, 2^{n/2}+1, 2^{n/2}-1\}$ [4] with dynamic range 4n and 5n propose high-performance reverse converters in addition to increasing parallelism. It should be noted that, modulo 2^n+1 in moduli set $\{2^{n/2}-1, 2^{n/2}+1, 2^n+1, 2^{2n+1}-1\}$ increases the execution delay in RNS arithmetic unit.

In this paper, the four-moduli set $\{2^{n+k}, 2^{2n-1}-1, 2^{n/2}+1, 2^{n/2}-1\}$ has been introduced and a high-speed two-level architecture reverse converter has been designed for it based on mix-radix conversion (MRC) algorithm. This moduli set provides a dynamic range between 4n to 5n and has a high-performance arithmetic unit due to its proper moduli. The proposed reverse converter has more speed in comparison to the similar moduli sets $\{2^{n/2}-1, 2^{n/2}+1, 2^n+1, 2^{2n+1}-1\}$ and $\{2^{2n}, 2^{2n+1}-1, 2^{n/2}+1, 2^{n/2}-1\}$.

2 Background

The RNS [1] is determined by a moduli set such as $\{m_1, m_2, \ldots, m_n\}$ in which all modulus are positive integers and pair wise relatively prime that make a dynamic range (DR) available in $[0, M)$ where M is calculated by:

$$M = \prod_{i=1}^{n} m_i. \tag{1}$$

Each integer X where $0 \leq X < M$, is a unique number in RNS that is represented by $(x_1, x_2, \ldots, x_n)$ such that:

$$x_i = X \bmod m_i = |X|_{m_i} \tag{2}$$

Mixed-radix conversion: for the 2-moduli set $\{m_1, m_2\}$ the number X can be converted from its residue representation (x_1, x_2) by MRC [1] as follows:

$$X = am_1 + x_1 \tag{3}$$

Where

$$a = \left| (x_2 - x_1) \left| m_1^{-1} \right|_{m_2} \right|_{m_2} \tag{4}$$

The $\left| m_1^{-1} \right|_{m_2}$ denotes the multiplicative inverse of m_1 modulo m_2.

DOI: 10.1587/elex.9.8
Received September 30, 2011
Accepted December 02, 2011
Published January 10, 2012

3 Designing the proposed reverse converter

To design an efficient reverse converter for flexible moduli set $\{2^{n+k}, 2^{2n-1}-1, 2^{n/2}+1, 2^{n/2}-1\}$, two-level architecture and MRC algorithm are used with respect to the corresponding residues (x_1, x_2, x_3, x_4). In the first level, two reverse converters for sub-sets $\{2^{n+k}, 2^{2n-1}-1\}$ and $\{2^{n/2}+1, 2^{n/2}-1\}$ are designed by considering their corresponding residues to obtain Z and Y respectively. Then, in the second level a reverse converter for moduli set $\{2^{n+k}(2^{2n-1}-1), 2^n-1\}$ is designed according to the results of the first level (Y, Z) to obtain the weighed number X.

3.1 Designing a reverse converter for moduli set $\{2^{n+k}, 2^{2n-1}-1\}$

With respect to the two-moduli set $\{m_1, m_2\} = \{2^{n+k}, 2^{2n-1}-1\}$ where $k <$ n, the binary number Z can be obtained from its corresponding residues (x_1, x_2) by MRC as follow:

$$Z = 2^{n+k}a_1 + x_1 \tag{5}$$

where

$$a_1 = |(x_2 - x_1)k_1|_{2^{2n-1}-1} \tag{6}$$

The multiplicative inverse of 2^{n+k} modulo $2^{2n-1}-1$ can be calculated as bellow:

$$\left|k_1 \times 2^{n+k}\right|_{2^{2n-1}-1} = 1 \rightarrow k_1 = 2^{n-k-1} \tag{7}$$

By substituting $k_1 = 2^{n-k-1}$ into (6) we have:

$$a_1 = \left|2^{n-k-1}(x_2 - x_1)\right|_{2^{2n-1}-1} \tag{8}$$

Eq. (8) can be simplified as follows:

$$a_1 = |v_2 + v_1|_{2^{2n-1}-1} \tag{9}$$

$$\begin{aligned} v_1 &= \left|-2^{n-k-1}x_1\right|_{2^{2n+1}-1} = \left|-2^{n-k-1}(\underbrace{0\ldots00}_{n-k-1}\underbrace{x_{1,n+k-1}\ldots x_{1,1}x_{1,0}}_{n+k})\right|_{2^{2n-1}-1} \\ &= \underbrace{\bar{x}_{1,n+k-1}\ldots\bar{x}_{1,1}\bar{x}_{1,0}}_{n+k}\underbrace{1\ldots11}_{n-k-1} \end{aligned} \tag{10}$$

$$\begin{aligned} v_2 &= \left|2^{n-k-1}x_2\right|_{2^{2n-1}-1} = \left|2^{n-k-1}(\underbrace{x_{2,2n-2}\ldots x_{2,1}x_{2,0}}_{2n-1})\right|_{2^{2n-1}-1} \\ &= \underbrace{x_{2,n+k-1}\ldots x_{2,1}x_{2,0}}_{n+k}\underbrace{x_{2,2n-2}\ldots x_{2,n+k}}_{n-k-1} \end{aligned} \tag{11}$$

3.2 Designing a reverse converter for moduli set $\{2^{n/2}+1, 2^{n/2}-1\}$

Initially, the multiplication inverse for two-moduli set $\{2^{n/2}+1, 2^{n/2}-1\}$ is determined as follow:

$$\left|k_2 \times (2^{n/2}+1)\right|_{2^{n/2}-1} = 1 \rightarrow k_2 = 2^{(n/2)-1} \tag{12}$$

DOI: 10.1587/elex.9.8
Received September 30, 2011
Accepted December 02, 2011
Published January 10, 2012

Next, with respect to the two-moduli set $\{2^{n/2}+1, 2^{n/2}-1\}$ the binary number Y, can be obtained from its corresponding residues (x_3, x_4) by substituting $m_3 = 2^{n/2}+1$, $m_4 = 2^{n/2}-1$ and the value of multiplicative inverse into (3)-(4) as below

$$Y = (2^{n/2}+1)a_2 + x_3 \tag{13}$$

$$a_2 = \left|2^{(n/2)-1}(x_4 - x_3)\right|_{2^{n/2}-1} \tag{14}$$

The Eq. (14) can be simplified as follow

$$a_2 = |v_4 + v_3|_{2^{n/2}-1} \tag{15}$$

Where

$$\begin{aligned} v_3 &= \left|2^{(n/2)-1}x_4\right|_{2^{n/2}-1} = \left|2^{(n/2)-1}(x_{4,(n/2)-1}\dots x_{4,1}x_{4,0})\right|_{2^{n/2}-1} \\ &= x_{4,0}\underbrace{x_{4,(n/2)-1}\dots x_{4,2}x_{4,1}}_{(n/2)-1} \end{aligned} \tag{16}$$

$$\begin{aligned} v_4 &= \left|-2^{(n/2)-1}x_3\right|_{2^{n/2}-1} = \left|-2^{(n/2)-1}(\underbrace{x_{3,n/2}\dots x_{3,1}x_{3,0}}_{(n/2)+1})\right|_{2^{n/2}-1} \\ &= \left|-2^{(n/2)-1}(x_{3,n/2}\times 2^{n/2} + \underbrace{x_{3,(n/2)-1}\dots x_{3,1}x_{3,0}}_{n/2})\right|_{2^{n/2}-1} \end{aligned} \tag{17}$$

Since the value of x_3 is in $0 \le x_3 < 2^{n/2}+1$ span, therefore this span can be divided as below

$$\begin{cases} 0 \le x_3 < 2^{n/2} & if \quad x_{3,n/2} = 0 \\ x_3 = 2^{n/2} & if \quad x_{3,n/2} = 1 \end{cases} \tag{18}$$

According to (18), Eq. (17) can be calculated as follow
If $x_{3,n/2} = 0$, we have

$$v_{41} = \left|-2^{(n/2)-1}(\underbrace{x_{3,(n/2)-1}\dots x_{3,1}x_{3,0}}_{n/2})\right|_{2^{n/2}-1} = \bar{x}_{3,0}\underbrace{\bar{x}_{3,(n/2)-1}\dots\bar{x}_{3,2}\bar{x}_{3,1}}_{(n/2)-1} \tag{19}$$

Else, if $x_{3,n/2} = 1$, we have

$$v_{42} = \left|-2^{(n/2)-1}\times 2^{n/2}(\underbrace{0\dots00}_{(n/2)-1}x_{3,n})\right|_{2^{n/2}-1} = 0\underbrace{1\dots11}_{(n/2)-1} \tag{20}$$

Therefore, v_4 is evaluated as

$$v_4 = \begin{cases} v_{41} & if \quad x_{3,n/2} = 0 \\ v_{42} & if \quad x_{3,n/2} = 1 \end{cases} \tag{21}$$

3.3 Designing a reverse converter for moduli set $\{2^{n+k}(2^{2n-1}-1), 2^n-1\}$

The multiplicative inverse for moduli set $\{2^{n+k}(2^{2n-1}-1), 2^n-1\}$ is calculated as below:

$$\left|k_3 \times 2^{n+k}(2^{2n-1}-1)\right|_{2^n-1} = 1 \rightarrow k_3 = 2^{n-k-1} \tag{22}$$

DOI: 10.1587/elex.9.8
Received September 30, 2011
Accepted December 02, 2011
Published January 10, 2012

For the moduli set $\{2^{n+k}(2^{2n-1}-1), 2^n-1\}$ where $k<n$, the final binary number X can be computed from its corresponding residues (Z,Y) by

$$X = Z + 2^{n+k}(2^{2n-1}-1)a_3 \tag{23}$$

where

$$a_3 = \left|2^{n-k-1}(Y-Z)\right|_{2^n-1} \tag{24}$$

By substituting (5) and (13) in (24), we have

$$a_3 = \left|2^{n-k-1}((2^{n/2}+1)a_2 + x_3 - 2^{n+k}a_1 - x_1)\right|_{2^n-1} \tag{25}$$

The above equation can be simplified as follow:

$$a_3 = |v_5 + v_6 + v_{71} + v_{72} + v_{81} + v_{82}|_{2^n-1} \tag{26}$$

where

$$\begin{aligned} v_5 &= \left|2^{n-k-1} \times (2^{n/2}+1)a_2\right|_{2^n-1} \\ &= \left|2^{n-k-1} \times (2^{n/2}+1)(\underbrace{0\ldots00}_{n/2}\underbrace{a_{2,(n/2)-1}\ldots a_{2,1}a_{2,0}}_{n/2})\right|_{2^n-1} \\ &= \left|2^{n-k-1}(\underbrace{a_{2,(n/2)-1}\ldots a_{2,1}a_{2,0}}_{n/2}\underbrace{a_{2,(n/2)-1}\ldots a_{2,1}a_{2,0}}_{n/2})\right|_{2^n-1} \end{aligned} \tag{27}$$

$$v_6 = \left|2^{n-k-1}x_3\right|_{2^n-1} = \left|2^{n-k-1}(\underbrace{0\ldots00}_{(n/2)-1}\underbrace{x_{3,n/2}\ldots x_{3,1}x_{3,0}}_{(n/2)+1})\right|_{2^n-1} \tag{28}$$

The equations (27) and (28) can be determined by $n-k-1$ bits circular left shift according to the value of k.

Since $|2^n|_{2-1}^n = 1$ so we have

$$\begin{aligned} v_7 &= \left|2^{n-k-1} \times -2^{n+k}a_1\right|_{2^n-1} = \left|-2^{n-1} \times 2^n a_1\right|_{2^n-1} \\ &= \left|-2^{n-1}(\underbrace{a_{1,2n-2}\ldots a_{1,1}a_{1,0}}_{2n-1})\right|_{2^n-1} \\ &= \left|-2^{n-1}(\underbrace{a_{1,2n-2}\ldots a_{1,n}}_{n-1} \times 2^n + \underbrace{a_{1,n-1}\ldots a_{1,1}a_{1,0}}_{n})\right|_{2^n-1} \end{aligned} \tag{29}$$

Eq. (31) can be separated into two parts as

$$v_{71} = \left|-2^{n-1}(\underbrace{a_{1,n-1}\ldots a_{1,1}a_{1,0}}_{n})\right|_{2^n-1} = \bar{a}_{1,0}\underbrace{\bar{a}_{1,n-1}\ldots\bar{a}_{1,2}\bar{a}_{1,1}}_{n-1} \tag{30}$$

$$v_{72} = \left|-2^{n-1} \times 2^n(0\underbrace{a_{1,2n-2}\ldots a_{1,n+1}a_{1,n}}_{n-1})\right|_{2^n-1} = \bar{a}_{1,n}\underbrace{1\bar{a}_{1,2n-2}\ldots\bar{a}_{1,n+1}}_{n-1} \tag{31}$$

DOI: 10.1587/elex.9.8
Received September 30, 2011
Accepted December 02, 2011
Published January 10, 2012

$$v_8 = \left|-2^{n-k-1}x_1\right|_{2^n-1} = \left|-2^{n-k-1}(\underbrace{x_{1,n+k-1}\ldots x_{1,1}x_{1,0}}_{n+k})\right|_{2^n-1} = \left|-2^{n-k-1}(\underbrace{x_{1,n+k-1}\ldots x_{1,n}}_{k}\times 2^n + \underbrace{x_{1,n-1}\ldots x_{1,1}x_{1,0}}_{n})\right|_{2^n-1} \quad (32)$$

The above equation can be divided in two parts as below

$$v_{81} = \left|-2^{n-k-1}(\underbrace{x_{1,n-1}\ldots x_{1,1}x_{1,0}}_{n})\right|_{2^n-1} = \underbrace{\bar{x}_{1,k}\ldots\bar{x}_{1,1}\bar{x}_{1,0}}_{k+1}\underbrace{\bar{x}_{1,n-1}\ldots\bar{x}_{k+1}}_{n-k-1} \quad (33)$$

$$v_{82} = \left|-2^{n-k-1}\times 2^n(\underbrace{0\ldots00}_{n-k}\underbrace{x_{1,n+k-1}\ldots x_{1,n+1}x_{1,n}}_{k})\right|_{2^n-1} \quad (34)$$

$$= \underbrace{1\bar{x}_{1,n+k-1}\ldots\bar{x}_{1,n+1}\bar{x}_{1,n}}_{k+1}\underbrace{1\ldots11}_{n-k-1}$$

Now, by letting the value of Z in (23) we have

$$X = x_1 + 2^{n+k}(a_1 + (2^{2n-1}-1)a_3) \quad (35)$$

The Eq. (35) can be simplified as follow

$$X = x_1 + 2^{n+k}W \quad (36)$$

where

$$W = T - H \quad (37)$$

$$T = 2^{2n-1}a_3 + a_1 = \underbrace{a_{3,n-1}\ldots a_{3,1}a_{3,0}}_{n}\underbrace{a_{1,2n-2}\ldots a_{1,1}a_{1,0}}_{2n-1} \quad (38)$$

$$H = a_3 = \underbrace{a_{3,n-1}\ldots a_{3,1}a_{3,0}}_{n} \quad (39)$$

Finally, subtraction (37) can be rewritten as follow addition operation:

$$\begin{array}{rl} T: & a_{3,n-1}...a_{3,1}a_{3,0}a_{1,2n-2}...a_{1,n}\ a_{1,n-1}...a_{1,1}a_{1,0} \\ +\bar{H}: & 11.....11\ \bar{a}_{3,n-1}...\bar{a}_{3,1}\bar{a}_{3,0} \\ + & \underline{00.....0\ \ 1} \\ W: & w_{3n-2}.....w_{n-1}w_n\ w_{n-1}.....w_1\ w_0 \end{array} \quad (40)$$

4 Hardware implementation

The required hardware to implement the proposed reverse converter is based on the equations (9), (15), (26) and (40). In this paper, to calculate (9) and (15), (2n − 1)-bits CPA with EAC and (n/2) bits CPA with EAC are used respectively. Also, a six-operand modulo $(2^n - 1)$ adder [5] is used to implement (26) that consists of four n-bit CSA with EAC followed by a n-bit CPA with EAC. According to (40), for calculating the n less significant bits of W, n NOT gates and an n-bit regular CPA (CPA4) with carry-in

DOI: 10.1587/elex.9.8
Received September 30, 2011
Accepted December 02, 2011
Published January 10, 2012

digit '1' is required. The remained $(2n-1)$ more significant bits of W are determined with respect to the carry-out bit of CPA4 such that if Cout $= 1$, these $(2n-1)$ bits are equal to the $(2n-1)$ more significant bits of T and if Cout $= 0$, the $(2n-1)$ more significant bits of W can be obtained by a

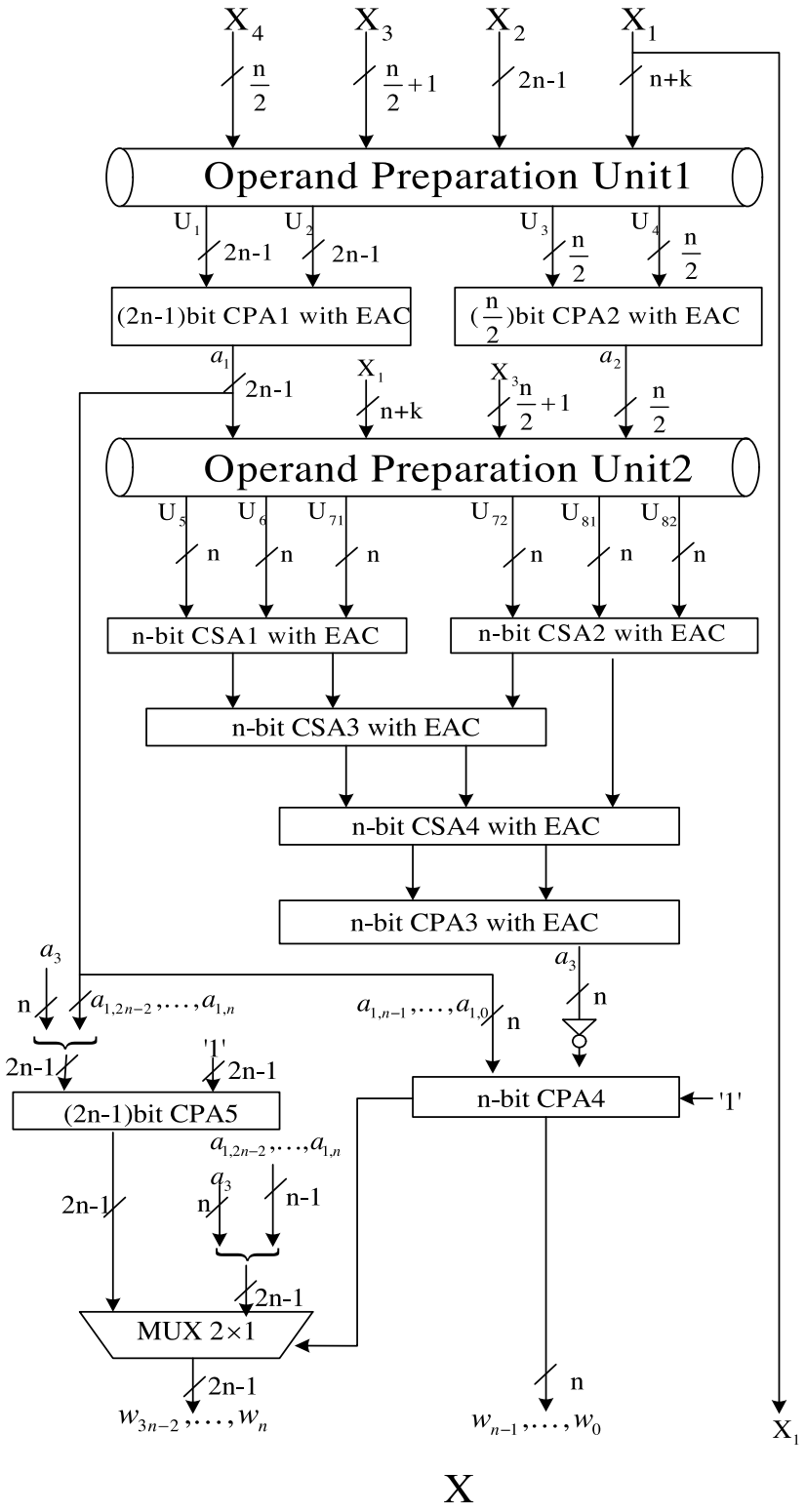

Fig. 1. The proposed converter for moduli set $\{2^{n+k}, 2^{2n-1}-1, 2^{n/2}+1, 2^{n/2}-1\}$

DOI: 10.1587/elex.9.8
Received September 30, 2011
Accepted December 02, 2011
Published January 10, 2012

$(2n-1)$-bit regular CPA (CPA5). Since all the $(2n-1)$ more significant bits of $\bar{H}$ are equal to the constant value '1', therefore all full adders in CPA4 can be reduced to the pair of XNOR/OR gates. Finally, equations (36) and (38) are obtained by a simple concatenation and no more hardware is required. Fig. 1 shows the hardware architecture of the proposed reverse converter.

5 Performance evaluation

Since the four-moduli set $\{2^{n+k}, 2^{2n-1}-1, 2^{n/2}+1, 2^{n/2}-1\}$ provides a flexible dynamic range between 4n to 5n bit, in this section we just compare it with the similar recently introduced four-moduli sets $\{2^{n/2}-1, 2^{n/2}+1, 2^n+1, 2^{2n+1}-1\}$ and $\{2^{2n}, 2^{2n+1}-1, 2^{n/2}+1, 2^{n/2}-1\}$ which offers 4n-bit and 5n-bit dynamic range respectively. In Table I, the proposed reverse converter has been compared with the introduced converters in [3] and [4] in terms of delay and hardware cost. To calculate the overall delay of the proposed converter, it should be considered that CPA1 and CPA2 as well as CPA4 and CPA5 operate in parallel. The delay of CPA1 and CPA2 is equal to $(4n-2)t_{FA}$ and nt_{FA} (t_{FA} refers to the delay of one full adder) respectively and hence, for calculating the overall delay, the delay of CPA1 has been considered. Also, the delay of CPA4 and CPA5 is equal to nt_{FA} and $(2n-1)t_{XNOR}$ respectively. To have a fair comparison between CPA4 and CPA5 delays, the unit gate model [6] is used. In this model, a FA and a XNOR gate have the delay of four and two unit gates. According to this, CPA4 and CPA5 have the delay of 4n and $4n-2$ unit gates respectively. Therefore, in calculating the overall delay, the delay of CPA4 has been considered. As it can be observed in Table I, the proposed converter has more performance in comparison to the introduced converters in [3] and [4].

Table I. Performance Comparison

Converter	FA	XNOR/OR pair	XOR/AND pair	NOT	Others	Conversion delay
[3]	8n+7	4n−3	2n−3	6n+4	–	$(8n+4)t_{FA}+2t_{NOT}$
[4]	7n+2	3n+1	0.5n−1	7.5n−1	MUX	$(9n+8)t_{FA}+3t_{NOT}+t_{MUX}$
Proposed	6n+2k	4n−2k−1	0.5n−1	5.5n+2k−1	MUX	$(7n+1)t_{FA}+3t_{NOT}+t_{MUX}$

6 Conclusion

In this paper, a high-speed two-level converter for flexible four-moduli set $\{2^{n+k}, 2^{2n-1}-1, 2^{n/2}+1, 2^{n/2}-1\}$ has been designed. The architecture of the proposed converter is just based on carry save adder and modular adder and hence, can be simply implemented by VLSI circuits. Comparison to the similar four-moduli sets $\{2^{n/2}-1, 2^{n/2}+1, 2^n+1, 2^{2n+1}-1\}$ and $\{2^{2n}, 2^{2n+1}-1, 2^{n/2}+1, 2^{n/2}-1\}$ shows that the proposed converter has more efficiency.

DOI: 10.1587/elex.9.8
Received September 30, 2011
Accepted December 02, 2011
Published January 10, 2012