ELectronics EXpress

IEICE Electronics Express, Vol.6, No.14, 1006–1012

A new five-moduli set for efficient hardware implementation of the reverse converter

Amir Sabbagh Molahosseini[1a)], **Chitra Dadkhah**[2], **and Keivan Navi**[3]

[1] *Department of Computer Engineering, Science and Research Branch, Islamic Azad University, Tehran, Iran*

[2] *Department of Electrical Engineering, K. N. Toosi University of Technology, Tehran, Iran*

[3] *Department of Electrical and Computer Engineering, Shahid Beheshti University, GC, Tehran, Iran*

a) *amir.sabbagh@srbiau.ac.ir*

Abstract: In this paper, we propose an efficient hardware implementation of the reverse converter for the new five-moduli set $\{2^n, 2^{n/2}-1, 2^{n/2}+1, 2^n+1, 2^{2n-1}-1\}$ for even n. The converter has a two-level architecture, and is based on combination of new Chinese remainder theorem 1 (New CRT-I) and mixed-radix conversion (MRC). The presented reverse converter has lower hardware requirements, and results in a significant reduction in the conversion delay, compared to the reverse converter of the latest introduced five-moduli set $\{2^n-1, 2^n, 2^n+1, 2^{n-1}-1, 2^{n+1}-1\}$ that has the same dynamic range as the proposed five-moduli set.

Keywords: reverse converter, residue arithmetic, VLSI architectures

Classification: Integrated circuits

References

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

[2] A. S. Molahosseini, K. Navi, O. Hashemipour, and A. Jalali, "An efficient architecture for designing reverse converters based on a general three-moduli set," *Elsevier J. Syst. Architecture*, vol. 54, no. 10, pp. 929–934, 2008.

[3] M. Hosseinzadeh, A. S. Molahosseini, and K. Navi, "An improved reverse converter for the moduli set $\{2^n-1, 2^n, 2^n+1, 2^{n+1}-1\}$," *IEICE Electron. Express*, vol. 5, no. 17, pp. 672–677, 2008.

[4] P. V. A. Mohan, "New reverse converters for the moduli set $\{2^n-3, 2^n-1, 2^n+1, 2^n+3\}$," *Elsevier J. Electron. Commun.*, vol. 62, no. 9, pp. 643–658, 2008.

[5] 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.

DOI: 10.1587/elex.6.1006
Received May 21, 2009
Accepted June 29, 2009
Published July 25, 2009

[6] Y. Wang, "Residue-to-Binary Converters Based on New Chinese remainder theorems," *IEEE Trans. Circuits Syst. II*, vol. 47, pp. 197–205, 2000.
[7] S. J. Piestrak, "Design of residue generators and multioperand modular adders using carry-save adders," *IEEE Trans. Comput.*, vol. 43, pp. 68–77, 1994.

1 Introduction

The residue number system (RNS) is a carry-free number system which can be used as a method for high-speed and low-power implementation of digital signal processing (DSP) computation algorithms [1]. The reverse conversion is very important and complex part of an RNS system. The complexity of the reverse converter is mainly based on moduli set. The most popular RNS moduli set is $\{2^n-1, 2^n, 2^n+1\}$ which has been attracted researchers for many decades. But, its dynamic range is inadequate for applications which require large dynamic range. Hence, newly, the general three-moduli set $\{2^\alpha, 2^\beta-1, 2^\beta+1\}$ [2] where $\alpha < \beta$, has been introduced for providing large dynamic range with low-complexity. Furthermore, four-moduli sets such as $\{2^n-1, 2^n, 2^n+1, 2^{n+1}-1\}$ [3] and $\{2^n-3, 2^n-1, 2^n+1, 2^n+3\}$ [4] have been considered for increasing parallelism. Nowadays, high-performance computation systems demand more parallelism with larger dynamic range. Thus, five-moduli sets are going under more development. The latest proposed five-moduli set is $\{2^n-1, 2^n, 2^n+1, 2^{n-1}-1, 2^{n+1}-1\}$ [5]. This set has balanced moduli, but its inefficient multiplicative inverses lead to performance degradation of the reverse converter.

In this paper, the new five-moduli set $\{2^n, 2^{n/2}-1, 2^{n/2}+1, 2^n+1, 2^{2n-1}-1\}$ for even n is introduced for RNS. This moduli set has simple multiplicative inverses which can lead to efficient design of reverse converter. Next, a two-level design of reverse converter for the proposed moduli set based on combination of New Chinese remainder theorem 1 (New CRT-I) and mixed-radix conversion (MRC) is presented. In comparison with reverse converter of the five-moduli set $\{2^n-1, 2^n, 2^n+1, 2^{n-1}-1, 2^{n+1}-1\}$ [5], the proposed converter has better performance in terms of hardware requirements and conversion delay.

2 Background

The RNS [1] is based on a moduli set $\{P_1, P_2, \ldots, P_n\}$ which consists of pairwise relatively prime numbers. The dynamic range is defined as $M = P_1P_2 \ldots P_n$. Each weighted number $X < M$ has a unique representation in RNS as $(x_1, x_2, \ldots, x_n)$ where

$$x_i = X \bmod P_i = |X|_{P_i}, \quad 0 \le x_i < P_i \tag{1}$$

DOI: 10.1587/elex.6.1006
Received May 21, 2009
Accepted June 29, 2009
Published July 25, 2009

By New CRT-I [6], the RNS number $(x_1, x_2, \ldots, x_n)$ can be converted into its equivalent weighted number as

$$X = x_1 + P_1 \left| k_1(x_2 - x_1) + k_2 P_2(x_3 - x_2) + \cdots + k_{n-1} P_2 P_3 \cdots P_{n-1}(x_n - x_{n-1}) \right|_{P_2 P_3 \cdots P_n} \quad (2)$$

Where $|k_1 \times P_1|_{P_2 P_3 \cdots P_n} = 1$, $|k_2 \times P_1 \times P_2|_{P_3 \cdots P_n} = 1$, …, $|k_{n-1} \times P_1 \times P_2 \times \cdots \times P_{n-1}|_{P_n} = 1$.

By MRC [1], the reverse conversion can be done as

$$X = z_n P_{n-1} \ldots P_2 P_1 + \ldots + z_3 P_2 P_1 + z_2 P_1 + z_1 \quad (3)$$

The mixed-radix digits can be calculated by $z_1 = x_1$, $z_2 = \left| (x_2 - z_1) \left| P_1^{-1} \right|_{P_2} \right|_{P_2}$, …, $z_n = \left| (((x_n - z_1) \left| P_1^{-1} \right|_{P_n} - z_2) \left| P_2^{-1} \right|_{P_n} - \cdots - z_{n-1}) \left| P_{n-1}^{-1} \right|_{P_n} \right|_{P_n}$. The term $\left| P_i^{-1} \right|_{P_j}$ denotes the multiplicative inverse of P_i modulo P_j

3 Reverse converter design

Consider the five-moduli set $\{2^n, 2^n + 1, 2^{n/2} + 1, 2^{n/2} - 1, 2^{2n-1} - 1\}$ with corresponding residues $(x_1, x_2, x_3, x_4, x_5)$. The proposed conversion algorithm consists of two levels. In the first level, the equivalent weighted number of the residues x_1, x_2, x_3 and x_4 is obtained by using New CRT-I based on subset $\{2^n, 2^n + 1, 2^{n/2} + 1, 2^{n/2} - 1\}$. Next, the result of the first level and x_5 are combined by using MRC, with respect to the set $\{2^n(2^n + 1)(2^{n/2} + 1)(2^{n/2} - 1), 2^{2n-1} - 1\}$.

3.1 Conversion equations for $\{2^n, 2^n + 1, 2^{n/2} + 1, 2^{n/2} - 1\}$ Based on New CRT-I:

The multiplicative inverses which are needed in (2), can be calculated as follows

$$|k_1 \times 2^n|_{2^{2n}-1} = 1 \rightarrow k_1 = 2^n \quad (4)$$

$$|k_2 \times 2^n \times (2^n + 1)|_{2^n - 1} = 1 \rightarrow k_2 = 2^{n-1} \quad (5)$$

$$\left| k_3 \times 2^n \times (2^n + 1) \times (2^{n/2} + 1) \right|_{2^{n/2}-1} = 1 \rightarrow k_3 = 2^{(n-4)/2} \quad (6)$$

The $Z = (x_1, x_2, x_3, x_4)$ can be obtained by substituting the values of multiplicative inverses, and moduli $P_1 = 2^n$, $P_2 = 2^n + 1$, $P_3 = 2^{n/2} + 1$, $P_4 = 2^{n/2} - 1$ in (2) as below

$$\begin{aligned} Z &= x_1 + 2^n \left| \begin{matrix} 2^n(x_2 - x_1) + 2^{n-1}(2^n + 1)(x_3 - x_2) \\ +2^{(n-4)/2}(2^n + 1)(2^{n/2} + 1)(x_4 - x_3) \end{matrix} \right|_{2^{2n}-1} \\ &= x_1 + 2^n \left| \begin{matrix} -2^n x_1 + (2^{n-1} - 2^{2n-1})x_2 + (2^{n-2}(2^n + 1) - 2^{(n-4)/2}(2^n + 1))x_3 \\ +2^{(n-4)/2}(2^n + 1)(2^{n/2} + 1)x_4 \end{matrix} \right|_{2^{2n}-1} \end{aligned} \quad (7)$$

The simplification of (7) can be performed with considering the point that, by expressing x_i in p bits, $\left| x_i \times 2^l \right|_{2^p - 1}$ and $|-x_i|_{2^p - 1}$ are equivalent to l bits

DOI: 10.1587/elex.6.1006
Received May 21, 2009
Accepted June 29, 2009
Published July 25, 2009

circular left shifting of x_i, and one's complement of x_i, respectively [1]. The residues can be represented at bit-level as: $x_1 = (x_{1,n-1}, \ldots, x_{1,1}, x_{1,0})$, $x_2 = (x_{2,n}, \ldots, x_{2,1}, x_{2,0})$, $x_3 = (x_{3,n/2}, \ldots, x_{3,1}, x_{3,0})$ and $x_4 = (x_{4,(n-2)/2}, \ldots, x_{4,1}, x_{4,0})$. Therefore, (7) can be rewritten as

$$Z = x_1 + 2^n Y \tag{8}$$

Where

$$Y = |Y_1 + Y_{21} + Y_{22} + Y_{31} + Y_{32} + Y_4|_{2^{2n}-1} \tag{9}$$

$$\begin{aligned} Y_1 &= |-2^n x_1|_{2^{2n}-1} = \left| -2^n (\underbrace{0\cdots00}_{n} \underbrace{x_{1,n-1}\cdots x_{1,1}x_{1,0}}_{n}) \right|_{2^{2n}-1} \\ &= \underbrace{\bar{x}_{1,n-1}\cdots\bar{x}_{1,1}\bar{x}_{1,0}}_{n} \underbrace{1\cdots11}_{n} \end{aligned} \tag{10}$$

$$\begin{aligned} Y_{21} &= \left|2^{n-1}x_2\right|_{2^{2n}-1} = \left| 2^{n-1} (\underbrace{0\cdots00}_{n-1} \underbrace{x_{2,n}\cdots x_{2,1}x_{2,0}}_{n+1}) \right|_{2^{2n}-1} \\ &= \underbrace{x_{2,n}\cdots x_{2,1}x_{2,0}}_{n+1} \underbrace{0\cdots00}_{n-1} \end{aligned} \tag{11}$$

$$\begin{aligned} Y_{22} &= \left|-2^{2n-1}x_2\right|_{2^{2n}-1} = \left| -2^{2n-1} (\underbrace{0\cdots00}_{n-1} \underbrace{x_{2,n}\cdots x_{2,1}x_{2,0}}_{n+1}) \right|_{2^{2n}-1} \\ &= \bar{x}_{2,0} \underbrace{1\cdots11}_{n-1} \underbrace{\bar{x}_{2,2n}\cdots\bar{x}_{2,2}\bar{x}_{2,1}}_{n} \end{aligned} \tag{12}$$

$$\begin{aligned} Y_{31} &= \left|2^{n-2}(2^n+1)x_3\right|_{2^{2n}-1} = \left| 2^{n-2}(2^n+1) (\underbrace{0\cdots00}_{(n-2)/2} \underbrace{x_{3,n/2}\cdots x_{3,1}x_{3,0}}_{(n+2)/2}) \right|_{2^{2n}-1} \\ &= \left| 2^{n-2} (\underbrace{0\cdots00}_{(n-2)/2} \underbrace{x_{3,n/2}\cdots x_{3,1}x_{3,0}}_{(n+2)/2} \underbrace{0\cdots00}_{(n-2)/2} \underbrace{x_{3,n/2}\cdots x_{3,1}x_{3,0}}_{(n+2)/2}) \right|_{2^{2n}-1} \\ &= x_{3,1}x_{3,0} \underbrace{0\cdots00}_{(n-2)/2} \underbrace{x_{3,n/2}\cdots x_{3,1}x_{3,0}}_{(n+2)/2} \underbrace{0\cdots00}_{(n-2)/2} \underbrace{x_{3,n/2}\cdots x_{3,3}x_{3,2}}_{(n-2)/2} \end{aligned} \tag{13}$$

$$\begin{aligned} Y_{32} &= \left|-2^{(n-4)/2}(2^n+1)x_3\right|_{2^{2n}-1} \\ &= \left| -2^{(n-4)/2} (\underbrace{0\cdots00}_{(n-2)/2} \underbrace{x_{3,n/2}\cdots x_{3,1}x_{3,0}}_{(n+2)/2} \underbrace{0\cdots00}_{(n-2)/2} \underbrace{x_{3,n/2}\cdots x_{3,1}x_{3,0}}_{(n+2)/2}) \right|_{2^{2n}-1} \\ &= 1 \underbrace{\bar{x}_{3,n/2}\cdots\bar{x}_{3,1}\bar{x}_{3,0}}_{(n+2)/2} \underbrace{1\cdots11}_{(n-2)/2} \underbrace{\bar{x}_{3,n/2}\cdots\bar{x}_{3,1}\bar{x}_{3,0}}_{(n+2)/2} \underbrace{1\cdots11}_{(n-4)/2} \end{aligned} \tag{14}$$

DOI: 10.1587/elex.6.1006
Received May 21, 2009
Accepted June 29, 2009
Published July 25, 2009

$$
\begin{aligned}
Y_4 &= \left|2^{(n-4)/2}(2^n+1)(2^{n/2}+1)x_4\right|_{2^{2n}-1} \\
&= \left|2^{(n-4)/2}(2^n+1)(2^{n/2}+1)(\underbrace{x_{4,(n-2)/2}\cdots x_{4,1}x_{4,0}}_{n/2})\right|_{2^{2n}-1} \\
&= \left|2^{(n-4)/2}(2^n+1)(\underbrace{x_{4,(n-2)/2}\cdots x_{4,1}x_{4,0}}_{n/2}\underbrace{x_{4,(n-2)/2}\cdots x_{4,1}x_{4,0}}_{n/2})\right|_{2^{2n}-1} \\
&= \left|2^{(n-4)/2}(\underbrace{x_{4,(n-2)/2}\cdots x_{4,1}x_{4,0}}_{n/2}\underbrace{x_{4,(n-2)/2}\cdots x_{4,1}x_{4,0}}_{n/2}\right. \\
&\qquad \left.\underbrace{x_{4,(n-2)/2}\cdots x_{4,1}x_{4,0}}_{n/2}\underbrace{x_{4,(n-2)/2}\cdots x_{4,1}x_{4,0}}_{n/2})\right|_{2^{2n}-1} \\
&= x_{4,1}x_{4,0}\underbrace{x_{4,(n-2)/2}\cdots x_{4,1}x_{4,0}}_{n/2}\underbrace{x_{4,(n-2)/2}\cdots x_{4,1}x_{4,0}}_{n/2} \\
&\qquad \underbrace{x_{4,(n-2)/2}\cdots x_{4,1}x_{4,0}}_{n/2}\underbrace{x_{4,(n-2)/2}\cdots x_{4,3}x_{4,2}}_{(n-4)/2}
\end{aligned} \tag{15}
$$

3.2 Conversion equations for $\{2^n(2^{2n}-1), 2^{2n-1}-1\}$ Based on MRC:

The MRC for these two moduli requires only one multiplicative inverse as

$$\left|k \times 2^n(2^{2n}-1)\right|_{2^{2n-1}-1} = 1 \rightarrow k = 2^{n-1} \tag{16}$$

Therefore, with considering (3), the $X = (Z, x_5)$ can be calculated based on the two-moduli set $\{2^n(2^{2n}-1), 2^{2n-1}-1\}$ as follows

$$X = Z + 2^n(2^{2n}-1)\left|(x_5 - Z)2^{n-1}\right|_{2^{2n-1}-1} \tag{17}$$

The binary vectors Z and x_5 can be represented in bit-level as $Z = (Z_{3n-1}, \ldots, Z_1, Z_0)$ and $x_5 = (x_{5,2n-2}, \ldots, x_{5,1}, x_{5,0})$. Now, (17) can be simplified as below

$$X = Z + 2^n(2^{2n}-1)T = \underbrace{Z + 2^{3n}T}_{(5n-1)\text{bits}} - 2^nT \tag{18}$$

$$T = |T_1 + T_{21} + T_{22}|_{2^{2n-1}-1} \tag{19}$$

Where

$$
\begin{aligned}
T_1 &= \left|2^{n-1}x_5\right|_{2^{2n-1}-1} = \left|2^{n-1}(\underbrace{x_{5,2n-2}\cdots x_{5,1}x_{5,0}}_{2n-1})\right|_{2^{2n-1}-1} \\
&= \left|2^{n-1}(\underbrace{x_{5,2n-2}\cdots x_{5,n+1}x_{5,n}}_{n-1}\underbrace{x_{5,n-1}\cdots x_{5,1}x_{5,0}}_{n})\right|_{2^{2n-1}-1} \\
&= \underbrace{x_{5,n-1}\cdots x_{5,1}x_{5,0}}_{n}\underbrace{x_{5,2n-2}\cdots x_{5,n+1}x_{5,n}}_{n-1}
\end{aligned} \tag{20}
$$

DOI: 10.1587/elex.6.1006
Received May 21, 2009
Accepted June 29, 2009
Published July 25, 2009

$$Z=\underbrace{Z_{3n-1}\cdots Z_1Z_0}_{3n}=\underbrace{Z_{3n-1}\cdots Z_{2n}Z_{2n-1}}_{n+1}\times 2^{2n-1}+\underbrace{Z_{2n-2}\cdots Z_1Z_0}_{2n-1} \quad (21)$$

$$\begin{aligned} T_{21} &= \left| -2^{n-1}\times 2^{2n-1}(\underbrace{0\cdots 00}_{n-2}\underbrace{Z_{3n-1}\cdots Z_{2n}Z_{2n-1}}_{n+1}) \right|_{2^{2n-1}-1} \\ &= \underbrace{\bar{Z}_{3n-2}\cdots\bar{Z}_{2n}\bar{Z}_{2n-1}}_{n}\underbrace{1\cdots 11}_{n-2}\bar{Z}_{3n-1} \end{aligned} \quad (22)$$

$$\begin{aligned} T_{22} &= \left| -2^{n-1}(\underbrace{Z_{2n-2}\cdots Z_1Z_0}_{2n-1}) \right|_{2^{2n-1}-1} \\ &= \left| -2^{n-1}(\underbrace{Z_{2n-2}\cdots Z_{n+1}Z_n}_{n-1}\underbrace{Z_{n-1}\cdots Z_1Z_0}_{n}) \right|_{2^{2n-1}-1} \\ &= \underbrace{\bar{Z}_{n-1}\cdots\bar{Z}_1\bar{Z}_0}_{n}\underbrace{\bar{Z}_{2n-2}\cdots\bar{Z}_{n+1}\bar{Z}_n}_{n-1} \end{aligned} \quad (23)$$

3.3 Hardware Implementation:

The proposed 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 based on equations (8), (9), (18) and (19). The implementation of (9) requires a six-operand modulo $(2^{2n}-1)$ adder. In this paper, we consider the method of [7] for implementation of multi-operand modular adders. Hence, the six-operand modulo $(2^{2n}-1)$ adder relies on a $2n$-bit six-input carry-save adder (CSA) tree followed by a $2n$-bit carry-propagate adder (CPA) with end-around carry (EAC). The six-input CSA tree consists of four $2n$-bit CSAs with EAC. Also, some of the full adders (FAs) in these CSAs are reduced to pairs of XNOR/OR or XOR/AND gates, because the operands (10)-(14) have some bits with the constant values of 0 or 1. Since, x_1 is an n-bit number, (8) can be realized with only concatenation of x_1 and Y, without the use of hardware. The implementation of (19) is also based on a $(2n-1)$-bit CSA with EAC followed by a $(2n-1)$-bit CPA with EAC. Next, realization of (18) relies on a $(5n-1)$-bit binary subtracter which can be implemented by a $(5n-1)$-bit regular CPA with '1' carry-in, and $(2n-1)$ NOT gates. It should be noted that, the term $Z+2^{3n}T$ is only a concatenation, because Z is a $3n$-bit number. Fig. 1 shows the hardware architecture of the converter.

4 Performance evaluation

Table I makes a comparison in terms of area and delay between the proposed reverse converter for the moduli set $\{2^n, 2^{n/2}-1, 2^{n/2}+1, 2^n+1, 2^{2n-1}-1\}$ and the converter of the moduli set $\{2^n-1, 2^n, 2^n+1, 2^{n-1}-1, 2^{n+1}-1\}$ [5]. Both these moduli sets have five moduli and the same dynamic range. As stated in [4], the converter of [5] has a total delay of $(18n+l+2)t_{\mathrm{FA}}$, where t_{FA} denotes the delay of an FA. For a better comparison, the unit gate model is considered

DOI: 10.1587/elex.6.1006
Received May 21, 2009
Accepted June 29, 2009
Published July 25, 2009

to obtain total area and delay estimations. Based on this model, each two-input monotonic gate counts as one gate in area and delay, an XOR/XNOR gate counts as two gates in area and delay, and an FA has area of seven gates and delay of four gates [2, 3]. The corresponding total unit gate area and delay are presented in Table I. It is clear from the Table that the proposed converter results in significant reduction in area and delay, compared to the converter of [5].

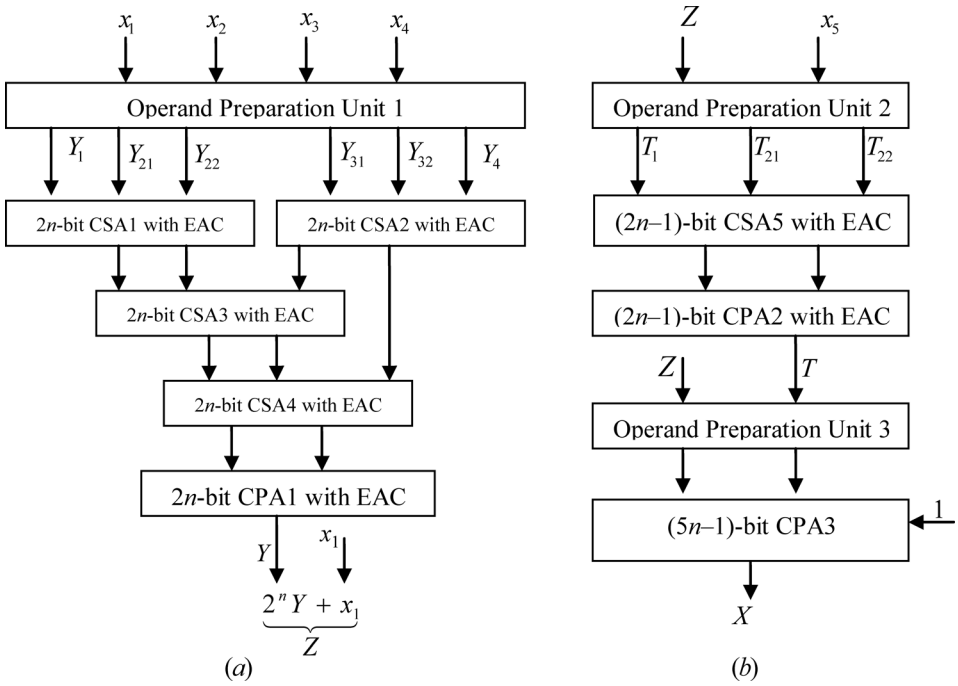

Fig. 1. The proposed reverse converter: (a) first level (b) second level

Table I. Performance Comparison

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

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

5 Conclusion

This paper presents an efficient two-level design of reverse converter for the new five-moduli set $\{2^n, 2^{n/2}-1, 2^{n/2}+1, 2^n+1, 2^{2n-1}-1\}$ based on combination of New CRT-I and MRC. Comparison with the latest five-modulus reverse converter has shown that the proposed design is faster and requires less hardware area.

DOI: 10.1587/elex.6.1006
Received May 21, 2009
Accepted June 29, 2009
Published July 25, 2009