International Academic Institute for Science and Technology

International Academic Journal of Science and Engineering
Vol. 2, No.1, 2015, pp.156-162.
ISSN 2454-3896

International Academic Journal of Science and Engineering

www.iaiest.com

Designing Reverse Converter for the New Three-Moduli Set {2^(2n+1),2^n-1,2^n+1}

Romina Shahbazi Youzband[a] , Mir kamal Mirnia[b]

[a] *Master student of Islamic Azad University of Tabriz.*

[b] *Associate Professor University of Tabriz.*

Abstract

Residue to binary Converter is the most complex steps of residue number system and it is also one of the factors that reduces the performance. In this paper efficient residue to binary converter is proposed for the new moduli set {2^(2n+1),2^n-1,2^n+1}. The proposed converter is designed by using the Chinese Remainder Theorem new-1 which includes a carry propagate adder (CPA) with end-around carry (EAC) and four carry save adder (CSA) with end-around carry (EAC).The proposed converter for moduli set {2^(2n+1),2^n-1,2^n+1} with 4n-bit dynamic range has better delay and hardware cost in comparison to the moduli set (Noorimehr et al, 2001) with the same dynamic range.

Keywords: Residue Number System (RNS), Fast Computing, New Chinese Remainder Theorem 1 (New CRT-I), Reverse Converter

Introduction:

In the conventional numerical system (binary, etc.) there is the carry propagation problem which reduces the performance computing hardware system. Residue number system is an unconventional number system that has been proposed in recent decades which is popular in the field of computing now. The computation in this system is carried out in parallel on the remainder of the original number which are smaller in comparison to the number in conventional representation. Thus, the computing speed will be increased and also the power will be reduced. (Szabo and Tanaka, 1967). Computations on independent modules are carried out in such a way that carry digit does propagate from one module to the other one (Parhami, 2000). Therefore, the basis or residue nimber systam is a worthifull tool for theoretical investigation of fast computation (Parhami, 2000).

The residue number system is used in many fields including RSA encryption algorithm (Cited et al, 2003), (Bajard and Imbert, 2004) and (Chen et al, 2013), a digital communications (Ramirez et al, 2002), error detection and correction (Yang and Hanzo, 2001), image processing (Wang et al, 2004) and etc. Many moduli moduli sets with 4n- bit dynamic range has been suggested so far including $\{2^{n/2}-1, 2^{n/2}+1, 2^n+1, 2^{2n+1}-1\}$ (Molahosseini et al, 2010), $\{2^n-1, 2^n, 2^n+1, 2^{n+1}-1\}$ (Mohan and Premkumar, 2007), $\{2^n-3, 2^n-1, 2^n+1, 2^n+3\}$ (Mohan, 2008) and $\{2^{2n}, 2^n+1, 2^{n/2}+1, 2^{n/2}-1\}$ (Noorimehr et al, 2014). In practice we may need a larger moduli sets like $\{2^n, 2^n-1, 2^n+1, 2^n-2^{(n+1)/2}+1, 2^n+2^{(n+1)/2}+1\}$, $\{2^{n+\beta}, 2^n-1, 2^n+1, 2^n-2^{(n+1)/2}+1, 2^n+2^{(n+1)/2}+1, 2^{n-1}+1\}$ and $\{2^{n+\beta}, 2^n-1, 2^n+1, 2^n-2^{(n+1)/2}+1, 2^n+2^{(n+1)/2}+1, 2^{n+1}+1\}$ which cover 5n bits dynamic ranges, 6n + β-1 bits and 6n + β + 1 bits respectively (Pettenghi et al, 2013).

In this paper, the residue to binary converter is given for the proposed moduli set by using the Chinese Remainder Theorem 1 in section 2. Hardware implementation of proposed converter is stated in section 3. Proposed converter is compared with the converter introduced in (Noorimehr et al, 2014) in the efficiency point of view and then a conclusion remark is stated in the last section.

Residue to Binary Conversion Algorithm

According to New Chinese Remainder Theorem-1 (Cao et al, 2003), for decoding from RNS representation into binary of the number X with the given residues $\langle x_1, x_2, x_3\rangle$, in moduli set $\{m_1, m_2, m_3\} = \{2^{2n+1}, 2^n-1, 2^n+1\}$ is obtained by

$$X = x_1 + m_1 |k_1(x_2 - x_1) + k_2 m_2 (x_3 - x_2)|_{m_2 m_3} \quad (1)$$

where

$$|k_1 \times m_1|_{m_2 m_3} = 1 \quad (2)$$

$$|k_2 \times m_1 \times m_2|_{m_3} = 1, \quad (3)$$ and k_1 and k_2 are the multiplicative inverses.

Binary representation of the residues $\langle x_1, x_2, x_3\rangle$, conrresponding to the moduli set $\{m_1, m_2, m_3\}$ is given by

$$x_1 = (x_{1,2n} \dots x_{1,1} x_{1,0}) \quad (4)$$

$$x_2 = (x_{2,n-1} \dots x_{2,1} x_{2,0}) \quad (5)$$

$$x_3 = (x_{3,n} \dots x_{3,1} x_{3,0}) \quad (6)$$

We show first that the modules are pairwise relatively prime in this moduli set. The following theorems are needed.

Theorem 1. The numbers $2^n + 1$, $2^n - 1$ and 2^{2n+1} are pairwise relatively prime.

Proof. According to the Euclid's theorem, we have

$$gcd(a, b) = gcd\ (b, a\ mod\ b) \qquad (7)$$

Note that $gcd(a, b)$ means the greatest common divisor of a and b. So we have

$$gcd(2^{2n+1}, 2^n - 1) = gcd(2^n - 1, 2) = 1 \qquad (8)$$
$$gcd(2^{2n+1}, 2^n + 1) = gcd(2^n + 1, 2) = 1 \qquad (9)$$
$$gcd(2^n + 1, 2^n - 1) = gcd(2^n - 1, 2) = 1. \qquad (10)$$

Theorem 2. The multiplicative inverse to (1) is $k_1 = 2^{2n-1}$ and $k_2 = 2^{n-2}$ respectively.

Proof. Let $m_1 = 2^{2n+1}$, $m_2 = 2^n - 1$ and $m_3 = 2^n + 1$. From (2) and (3) we have

$$|k_1 \times 2^{2n+1}|_{2^{2n}-1} \qquad (11)$$
$$= |2^{2n-1} \times 2^{2n+1}|_{2^{2n}-1}$$
$$= |2^{4n}|_{2^{2n}-1} = 1$$

$$|k_2 \times 2^{2n+1} \times 2^n - 1|_{2^n+1} \qquad (12)$$
$$= |2^{n-2} \times 2 \times (-2)|_{2^{2n}-1} = 1.$$

Now, for the moduli set $\{m_1, m_2, m_3\} = \{2^{2n+1}, 2^n - 1, 2^n + 1\}$, eq. (1) can be rewritten as

$$X = x_1 + 2^{2n+1}|2^{2n-1}(x_2 - x_1) + \qquad 2^{n-2}(2^n - 1)(x_3 - x_2)|_{2^{2n}-1}\ . \qquad (13)$$

To reduce the hardware complexity in implementation, the following two properties can be used for computing and simplifing (13).

Property 1. Multiplication of a residue number Modulo $(2^p - 1)$ by 2^k is equivalent to rotating the number *k* bits to the left , where *p* and *k* are positive integers, (Pettenghi et al, 2013).

Property 2. a negative number in modulo $(2^p - 1)$ is obtained by subtracting this number from $(2^p - 1)$, which is equivalent to taking the one's complement of this number (Pettenghi et al, 2013).

Eq. (13) can be simplified as

$$X = x_1 + 2^{2n+1}W \qquad (14)$$

where $W = |2^{2n-1}(x_2 - x_1) + 2^{n-2}(2^n - 1)(x_3 - x_2)|_{2^{2n}-1}$; then

$$W = |P_1 + P_{21} + P_{22} + P_{31} + P_{32}|_{2^{2n}-1} \qquad (15)$$
$$P_1 = |-2^{2n-1}x_1|_{2^{2n}-1} \qquad (16)$$
$$P_{21} = |2^{n-2}x_2|_{2^{2n}-1} \qquad (17)$$
$$P_{22} = |(2^{2n-1} - 2^{2n-2})x_2|_{2^{2n}-1} \qquad (18)$$

$$P_{31} = |2^{2n-2}x_3|_{2^{2n}-1} \quad (19)$$
$$P_{32} = |-2^{n-2}x_3|_{2^{2n}-1}. \quad (20)$$

From the propery 1 and propery 2, the relations (16) to (20) can be computed as follows. Since x_1 is a $2n+1$-bit number then P_1 can be written as

$$P_1 = |P_{11} + P_{12}|_{2^{2n}-1} \quad (21)$$

Which leads to

$$P_{11} = \left|-2^{2n-1}(\underbrace{x_{1,2n-1}\dots x_{1,1}x_{1,0}}_{2n})\right|_{2^{2n}-1} = \underbrace{\bar{x}_{1,0}\bar{x}_{1,2n-1}\dots\bar{x}_{1,1}}_{2n}$$

$$P_{12} = \left|-2^{2n-1}(\underbrace{0000\ \dots\ \dots x_{1,2n}}_{2n})\right|_{2^{2n}-1} = \underbrace{\bar{x}_{1,2n}\dots\dots 1111}_{2n}$$

$$\begin{aligned} P_{21} &= |2^{n-2}x_2|_{2^{2n}-1} \\ &= \left|2^{n-2}(\underbrace{x_{2,n-1}\dots x_{2,1}x_{2,0}}_{n})\right|_{2^{2n}-1} \\ &= \left|2^{n-2}(\underbrace{0\dots 00}_{n}\ \underbrace{x_{2,n-1}\dots x_{2,1}x_{2,0}}_{n})\right|_{2^{2n}-1} \\ &= 00\ \underbrace{x_{2,n-1}\dots x_{2,1}x_{2,0}}_{n}\ \underbrace{0\dots 00}_{n-2} \end{aligned} \quad (22)$$

$$\begin{aligned} P_{22} &= |(2^{2n-1}-2^{2n-2})x_2|_{2^{2n}-1} \\ &= |(2^{2n-2})x_2|_{2^{2n}-1} \\ &= \left|2^{2n-2}(\underbrace{x_{2,n-1}\dots x_{2,1}x_{2,0}}_{n})\right|_{2^{2n}-1} \\ &= \left|2^{2n-2}(\underbrace{0\dots 00}_{n}\ \underbrace{x_{2,n-1}\dots x_{2,1}x_{2,0}}_{n})\right|_{2^{2n}-1} \\ &= x_{2,1}x_{2,0}\ \underbrace{0\dots 00}_{n}\ \underbrace{x_{2,n-1}\dots x_{2,2}}_{n-2} \end{aligned} \quad (23)$$

$$\begin{aligned} P_{31} &= |2^{2n-2}x_3|_{2^{2n}-1} \\ &= \left|2^{2n-2}(\underbrace{x_{3,n}\dots x_{3,1}x_{3,0}}_{n+1})\right|_{2^{2n}-1} \end{aligned}$$

$$= \left| 2^{2n-2}(\underbrace{0 \dots 00}_{n-1}\ \underbrace{x_{3,n} \dots x_{3,1}x_{3,0}}_{n+1}) \right|_{2^{2n}-1}$$
$$= x_{3,1}x_{3,0}\underbrace{0 \dots 00}_{n-1}\ \underbrace{x_{3,n} \dots x_{3,2}}_{n-1} \qquad (24)$$

$$P_{32} = |-2^{n-2}x_3|_{2^{2n}-1}$$
$$= \left| -2^{n-2}(\underbrace{x_{3,n} \dots x_{3,1}x_{3,0}}_{n+1}) \right|_{2^{2n}-1}$$
$$= \left| -2^{n-2}(\underbrace{0 \dots 00}_{n-1}\ \underbrace{x_{3,n} \dots x_{3,1}x_{3,0}}_{n+1}) \right|_{2^{2n}-1}$$
$$= 1\underbrace{\bar{x}_{3,n} \dots \bar{x}_{3,1}\bar{x}_{3,0}}_{n+1}\underbrace{1 \dots 11}_{n-2} \qquad (25)$$

Therefore, *X* in (14) is in the following form

$$X = x_1 + 2^{2n+1}W$$
$$= \underbrace{W_{2n-1} \dots W_1 W_0}_{2n}\ \underbrace{x_{1,2n} \dots x_{1,1}x_{1,0}}_{2n+1} \qquad (26)$$

Hardware Implementation

Hardware implementation of residue to binary converter proposed for moduli set $\{2^{2n+1}, 2^n - 1, 2^n + 1\}$ is shown in Fig. 1 which is based on (14) and (15). The required hardware for calculating (21) and (25) involves $(3n + 2)$ *NOT* gates in operand preparation unit (OPU). Implementing (15) requires a 6-operands adder which contains one $2n$-bit carry propagate adder (CPA) with end-around carry (EAC) and four $2n$-bit carry-save adder (CSA) with end-around carry. The values of (21)-(25) are either "0" or "1". Therefore some of full-Adders in these CSAs can be converted to the pair of XOR/AND or XNOR/OR gates. The delay of a CSA with EAC in

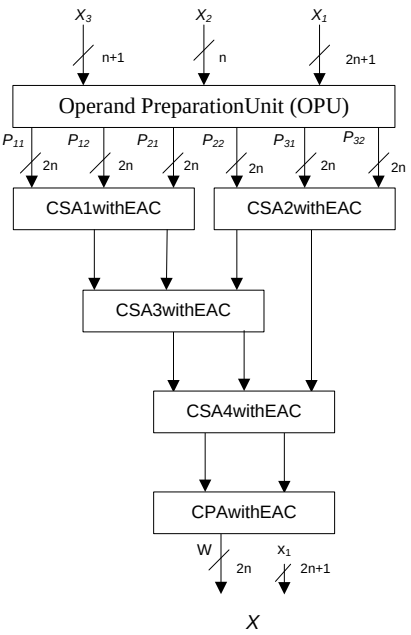

Figure 1- Residue to binary converter proposed for moduli set $\{2^{2n+1}, 2^n - 1, 2^n + 1\}$

this implementation is the same as that of a full adder and the delay of a CPA with EAC is twice of the delay of a regular CPA. Implemting $X = x_1 + 2^{2n+1}W$ does not require any extra hardware and we need only to concatenate W to x_1.

Performance Evaluation

The performance of the proposed reverse converter is evaluated by comparing it with other modules with the same dynamic range such as (Mohan and Premkumar, 2007), (Mohan, 2008), (Hosseinzadeh et al, 2008), (Molahosseini et al, 2010) and (Noorimehr et al, 2014). As it is shown in (Noorimehr et al, 2014), delay and hardware cost in $\{2^{2n}, 2^{n/2} - 1, 2^{n/2} + 1, 2^n + 1\}$ is better than the other converters such as (Mohan and Premkumar, 2007), (Mohan, 2008), (Hosseinzadeh et al, 2008), (Molahosseini et al, 2010). Therefore, the proposed converter is compared only with reverse converter in (Noorimehr et al, 2014). The delay and hardware costs needed in residue to binary converter in the moduli sets $\{2^{2n+1}, 2^n - 1, 2^n + 1\}$ and $\{2^{2n}, 2^{n/2} - 1, 2^{n/2} + 1, 2^n + 1\}$ are shown in table 1. The simulation results obtained by using ISE software, version 1.12 are shown in table 2. As it can be seen from table 2, the proposed converter needs less area as well as less delayin comparison with (Noorimehr et al, 2014) and thus it will be faster.

Conclusion

In this paper, the algorithm of residue to binary converter hase been introduced for moduli set $\{2^{2n+1}, 2^n - 1, 2^n + 1\}$. The proposed converter has been designed by using the New CRT-1 which involves a $2n$-bit CPA with EAC and four $2n$-bit CSA with EAC. By invetigating the results obtained, it seems that the proposed converter enjoy better performance by comparing to converter (Noorimehr et al, 2014).

References:

Bajard, J. C. and Imbert, L. (2004). Brief contributions: A Full Implementation RSA in RNS. IEEE Transactions on Computer. Vol. 53. No. 6. 769-774.

Cao, B., Chang, C. H. and Srikanthan, T. (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. 1296–1303.

Chang,C. H. and Srikanthan,T. (2003). Adder based residue to binary converters for a new balanced 4-moduli set, in Proc. 3rd IEEE Symp. Image. Signal Process. Anal. Vol. 2. 820–825.

Chen, C. S., Wang, T. and Tian, J. (2013). Improving timing attack on RSA-CRT via error detection and correction strategy. Information Sciences. Vol. 232. 464–474.

Ciet, M., Nevel, M., Peetersl, E. and Quisquater, J. J. (2003). Parallel FPGA implementation of RSA with residue number systems. Proceedings of the 46th IEEE International Midwest Symposium on Circuits and Systems. Vol. 2. 806-810.

Hosseinzadeh, M., Molahosseini, A. S. and Navi, K. (2008). An improved reverse converter for the moduli set {2^n –1,2^n,2^n+1,2^(n+1)–1}. IEICE Electron. Exp. Vol. 5. No. 17. 672–677.

Mohan, P. V. A. (2008). New reverse converters for the moduli set {2^n –3,2^n –1,2^n+1,2^n+3}. Elsevier J. Electron. Commun. (AEU). Vol. 62. No. 9. 643–658.

Mohan, P. V. A. and Premkumar, A. B. (2007). RNS-to-binary converters for two four-moduli sets {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 Trans. Circuits Syst. I, Reg. Papers. Vol. 54. No. 6. 1245–1254.