ISSN No. 0976-5697

Volume 2, No. 1, Jan-Feb 2011

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

Improved 2^n-Modulo Multiplier in Residue Number System

Seyyed Mohammad Safi*
Islamic Azad University,
Ahvaz branch, Iran
sm.safi@iauahvz.ac.ir

Hadi Toofani
Islamic Azad University,
Tabriz branch, Iran
Hadi.toofani@gmail.com

Mahdi Mahmoodi
Islamic Azad University,
Ahvaz branch, Iran
m_mahmoodi_srb@ iauahvz.ac.ir

Misagh Mohammadizadeh
Department of Computer Engineering
Tehran Sciences and Researches unit
Iran Azad University
m.mohammadi@srbiau.ac.ir

Abstract: Residue number system (RNS) is a mathematical method to execute computing processes. In this method, the large operands which need more time to be calculated, convert to small ones to consume less time. In RNS, to decrease the delay time, some transistors used as a matrix to select output of operations in a transistor delay time.

In this paper, by using of one-hot system in RNS, the used hardware decreased to calculate the result of 2^n-modulo multiplication.

Index terms: One-hot, RNS multiplier

I. BACKGROUND

Residue Number Systems (RNS) are parallel weight-less number systems which are based on modular arithmetic by using of relatively prime numbers called moduli. The product of these moduli is equal to the dynamic range of the RNS. One important advantage of the RNS is that each residue digit is computed independently [1].

Recent analytical results have indicated that the One-Hot Residue (OHR) number system can reduce the delay-power product (DPP) of mathematical operation circuits when compared with those based on the binary number system [2]. Delay reduction is a consequence of the fact that addition and multiplication are performed by barrel shifters. Power reduction is due to the decreased switching activity factors of digits, which are encoded in the one-hot representation.

The recently developed OHR Number System offers just such a possibility. It possesses delay-power products which are significantly improved over the binary number system, and is ideally suited for high-speed portable applications.

In next section some of the RNS multipliers will be introduced briefly, and then the one-hot adder will be analyzed. In fourth section, the new proposed multiplication will be explained and finally, in last section, the conclusion of this paper is illustrated and the results compared with previous methods.

II. RNS MULTIPLIERS

Many RNS multiplier has been designed so far which are pur[1]e table-look-up multipliers, quarter square multipliers, index transform multipliers, and array multipliers [4]. In its simplest form, each modulo m_i multiplier can be implemented using ROMs or an array of full adder cells. Design using the ROM approach is based on a look-up table and is excellent for smaller moduli multipliers, however it takes up a lot of area as the magnitude of the number goes up. The ROM size increases exponentially with the number of bits in each operand. For a multiplier employing an array of full adder cells the delay is linear with the number of bits in each operand.

III. ONE-HOT ADDER

Modulo $m_i$addition is performed using an m_i*$m_i$barrel shifter because it is a cyclic permutation when the operands are one-hot encoded. The degradation is due to the threshold voltage drop across the pass transistors. Consequently, level restoration circuitry must be included on the output. This topic will be discussed below. Subtraction is implemented by transposing the subtrahend wires to generate its additive inverse modulo m_i. Note the simplicity with which the additive inverse is formed; no active circuitry is required. Figure 1 shows an OHR adder.

*This paper has been derived from seyyed mohammad safi research plan in Islamic Azad university Ahvaz branch.

© 2010, IJARCS All Rights Reserved

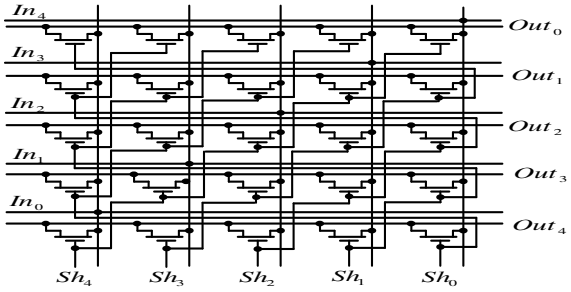

Figure 1: Modulo 5 OHRNS adder model.

IV. IMPROVED ADDER

In this paper, a new way proposed to increase the speed of 2^n-modulo multiplication. In this way, the product of multiplication is achieved by new algorithm and calculation will be done by OHR. In this method, the result of multiplication calculated by some of the small sum. For better result, we use one-hot adder to calculate sum results which have one-transistor delay. It is asserted that in 2^n-modulo multiply we need n bit of result`s least important bits. Figure 2 shows the result of 2^n -modulo multiplication in previous method which has n^2 delay.

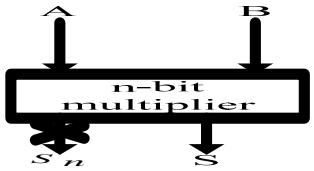

Figure 2: Traditional RNS $\mathbf{2^n}$-modulo Multiplier

In order to decrease the delay of the operation, we use OHR in multiplication steps. For this purpose, an OHR matrix which designed for 2^n-modulo multiplication will be used. As shown in figure 3, digits of operands will be multiplied by OHR, and results gathered in columns and will be add by OHR adder. Because of parallel operations in this system the delay of this calculation will be increased to two transistors. First is for multiplication and second for addition.

For achieving of A multiplication by B, we consider each of them as two part: High order and low order as shown in equation 1.

On this base:

$$
\begin{aligned}
&m = r^n \Rightarrow\ 0 \le A < m = r^n \\
&A = \left(a_{n-1} \dots\ a_{(n/2)} a_{(n/2)-1} \dots\ a_2 a_1 a_0\right)_r = \alpha_1 \alpha_0 \\
&(\alpha_1)_{P_2} = \left(a_{n-1} \dots\ a_{(n/2)}\right)_r \\
&(\alpha_0)_{P_1} = \left(a_{(n/2)-1} \dots\ a_2 a_1 a_0\right)_r \\
&B = \left(b_{n-1} \dots\ b_{(n/2)} b_{(n/2)-1} \dots\ b_2 b_1 b_0\right)_r = \beta_1 \beta_0 \\
&(\beta_1)_{P_2} = \left(b_{n-1} \dots\ b_{(n/2)}\right)_r \\
&(\beta_0)_{P_1} = \left(b_{(n/2)-1} \dots\ b_2 b_1 b_0\right)_r \\
&P_1 = P_2 = r^{(n/2)}
\end{aligned}
\qquad (1)
$$

As ordinary multiplication, each part of operands is ultiplied and results add as shown in figure 3.

$$
\begin{array}{rcccc}
 & & \alpha_1 & \alpha_0 & \\
 & \times & \beta_1 & \beta_0 & \\
\hline
 & & \beta_0\alpha_1 & \beta_0\alpha_0 & \\
+ & \beta_1\alpha_1 & \beta_1\alpha_0 & & \\
\hline
 & Z_2 & Z_1 & Z_0 &
\end{array}
$$

Figure 3: ordinary multiplication steps

In the proposed method, multiplication operands divide to two parts and become smaller to use OHR as a fast way to get results. As shown in figure 3, for achieving A and B multiplication, we need n*n transistor OHR multiplier and in contrast, for α and β multiplication, it is needed $\frac{n}{2} * \frac{n}{2}$ transistor which means four times less hardware.

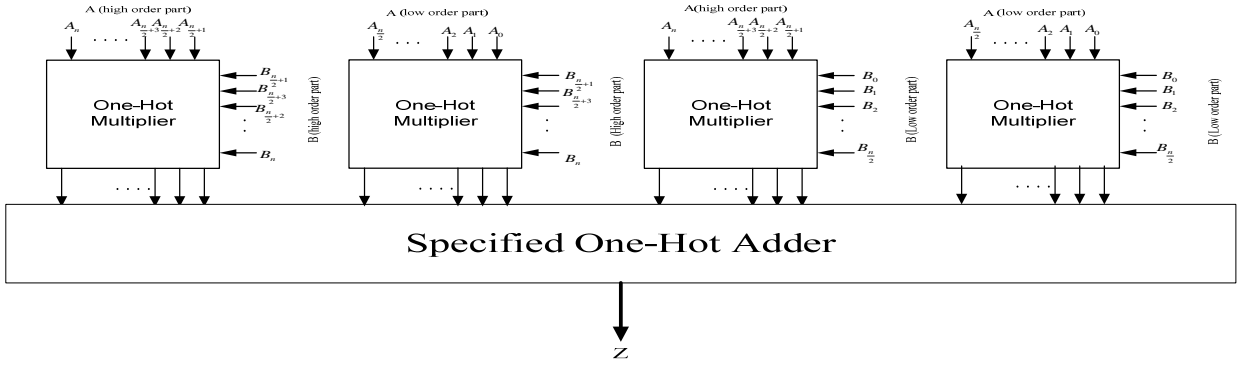

Figure 4: Improved One-hot $\mathbf{2^n}$-modulo Multiplier

After achieving of multiplication results, we add up the results to achieve final one. As mentioned in previous, some product`s most important bits are not needed and we can decrease the OHR adder size by using of needed bits calculation as shown in figure 4.

© 2010, IJARCS All Rights Reserved

V. CONCLUSION AND COMPARISON

In this paper, a new method is proposed to calculate the result of 2^n-modulo multiplication. In this method, the large circuits of multiplication are converted to smaller one-hot adders which have one transistor delay. The results show that the delay of calculation for 2^n-modulo multiplication is decreased to three transistor delay.

The One-Hot Residue Number System allows the implementation of high-speed simple adders and multipliers. The OHRNS is an effective way to mathematical operation but for large moduli calculation, the hardware area will be grown exponentially. By proposed way, multiplication calculation will be done in smaller area up to four times [7]. The compared results illustrated in table 1.

Table 1: Proposed Multiplier compared with [7]

	Delay (transistor)	Hardware (transistor)	Time complexity
[7]	1	2^{2n}	2^{2n}
Proposed OHRNS Multiplier	3	$4 * 2^n + 2n$	2^n

VI. REFERENCE

[1] A. Omondi and B. Premkumar,2007, "Residue Number System- theory and implementation," Imperial College Press.

[2] M. Hosseinzadeh, S. J. Jassbi and k. Navi, 2007, "A Novel Multiple Valued Logic OHRNS Modulo rn Adder Circuit," International Journal of Electronics, Circuits and Systems, Vol. 1, No. 4, pp. 245-249.

[3] M. Abdallah and A. Skavantzos, JULY 2005 Member, IEEE "On Multi Moduli Residue Number Systems With Moduli of Forms (, 1, 1) a b c r r − r + "IEEE TRANSACTIONS ON CIRCUITS AND SYSTEMS—I: REGULAR PAPERS, VOL. 52, NO. 7.

[4] F. J. Taylor, "Residue arithmetic: A tutorial with examples," IEEE Comput. Mag., vol. 17, pp. 50–62, May 1984.

[5] F.J. Taylor,"Large Moduli Multipliers for Signal Processing,"IEEE Trans. Circuits Syst., vol. CAS-28, pp. 731-736, July 1981.

[6] G.A. Jullien, "Implementation of Multiplication, Modulo a Prime Number, with Applications to Number Theoretic Transforms," IEEE Trans. Comput., vol. C-29, pp. 899-905, Oct. 1980.

[7] W. A. Chren, Jr., C. H. Brogdon and D. Andrevska, "Delay Power Product Simulation Results For One-Hot Residue Number System Arithmetic Circuits.", IEEE, 1997. Pp. 544-547

[7] H. Garner, "The Residue Number System," IEEE Transactions Electronic Computer, Vol. 8, pp.140-147, 1959.

[8] N. Szabo and R. Tanaka, Residue arithmetic and its applications to computer technology, (New York, McGraw-Hill, 1967).

[9] M. Hosseinzadeh, K. Navi and S. Timarchi, "Design Residue Number System Circuits in Current mode," 14th Iranian Conference of Electrical Engineering, 2006.

[10] M. Hosseinzadeh, K. Navi and S. Timarchi, "New Design of 4-3 Compressor," 11th International CSI Computer Conference of Iran, 2006.

© 2010, IJARCS All Rights Reserved