International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 3 Issue 11, November-2014

An Adder/Multiplier Circuit for OneHot Residue Number System

Mokhtar Mohammadi Ghanatghestani[1] , Behnam Ghavami [2], Hossein Pedram[3]
[1]Department of Computer Engineering, Science and Research Branch, Islamic Azad University,Tehran, Iran
[2]Shahid Bahonar University, Kerman, Iran
[3]Amirkabir University of Technology (Tehran Polytechnic), Tehran, Iran

***Abstract*—Residue Number System (RNS) is a non-weighted number system. Residue Number System can be performed parallel, fast, low power and secure arithmetic operations. Arithmetic operations in the Residue Number System, such as addition, subtraction and multiplication are executed high speed and in a short period of time without the need to propagation carry. Therefore RNS can be used for some of applications that require to high speed. For increase speed and reduce power consumption in the RNS a method has been proposed that named One-Hot Residue Number System. The delay arithmetic operation with using of this method is equivalent to a transistor, and power consumption in this method is minimal. The main problem with this method is the great increase in the number of transistors they are increased in order m2 (m is the module size). Hence OHRNS are suitable for small modules, and practically using this method is impossible for large modules. Proposed design of OHRNS in this paper generates many operations (such as addition, subtraction and multiplication) of two parameters synchronously, without hardware overhead compare to one original design of OHRNS.**

Keywords—Computer Arithmetic; one hot Adder/Multiplier; One-Hot Residue Number System (OHRNS); Residue Number System (RNS)

I. INTRODUCTION

Residue Number System is an integer, unconventional and non weighted number system. RNS can be supporting high speed and parallel arithmetic operation. In RNS, an integer is defined by a set of residue with shorter binary representations, which can be processed independently and in parallel. Because the arithmetic operations such as addition, subtraction and multiplication are able to execute in RNS very speed without the need to propagation carry, RNS arithmetic is used in the numeral real-time applications. The inherent fault tolerant properties of the residue number system can be able used for reliable and high performance applications.

The several applications of Residue Number System are as follows:

1-implementing DSP algorithm [1]

2-Image processing [1,2,3,4]

3-Numberal Filters [5,6]

4-Numberal Communication [7]

5-cryptography algorithm [8]

RNS architectures are also inherently fault tolerant against faults and easily provide fault detection and correction [9].

The important parameters in design and implementing the arithmetic circuits are hardware area, speed and power consumption of arithmetic units.

One-Hot is the method that this ability has created arithmetic operation in a RNS that can implementation of the system minimum power consumption and maximum speed. But other important parameter is hardware area in the implementation of arithmetic operation circuits. And hardware-based provider One-Hot is a barrel shifter, which is a regular and simple structure. Adders and multipliers are barrel shifter-based and, therefore, regular and simple.

Although the One-Hot the implementation arithmetic circuits is suitable for small modules. On the one hand in some applications need to the large dynamic ranges but for achieving a large dynamic range, must the increased in module size so number of transistors increased in order m^2 where m is the module size. If the selected module is m, then the amount of hardware in modular add or subtract in OHR using barrel shifter is in the order of m^2.This rate will cause problem when two or more barrel shifters are needed in the circuit. For example when we need both add and subtract operations then we have two barrel shifters. In this case amount of hardware is equal to $2m^2$. And if we need three operations (such as addition, subtraction and multiplication) amount of hardware is equal to $3m^2$. In this paper a new design for OHR add/multiply circuit is presented that generate both modular add and multiply results. In this design just one barrel Shifter structure is used.

The rest of this paper is organized as follows: argue about Residue Number System (RNS) in section II and One-Hot RNS (OHRNS) in section III. In section IV present design for one hot Adder/Multiplier. And compare proposed structure with basic OHRNS structure in section V, finally conclusion is in section VI.

II. RESIDUE NUMBER SYSTEM

Residue Number System is a non-conventional and non weighted number system. This System can be performed parallel, fast, low power and secure arithmetic operations.

RNS Advantage a cause which many used in the arithmetic applications such as numeral signal processing systems, image processing, Numeral Filters, implementing DSP algorithm, ad hoc networks and reliable systems is used. On for general is very used of RNS in the systems that usage that a range of numbers and applying addition, subtraction and multiplication of very is repeats.

Residue Number System is defined by moduli set such as$\{m_1, m_2, m_3, \dots, m_n\}$. All modules are positive integers and selection of modules is very important in the Residue Number System. also while all the modules are relatively pair wise prime the system will have the largest possible dynamic range which equals [α, α+M) in which α is an integer and M is:

$$M = \prod_{i=1}^{n} m_i \qquad (1)$$

Any integer X that α ≤ X< α+M in Residue Number System show by the set of reminder$(x_1, x_2, x_3, \dots, x_n)$ .and according to the following formula calculated remaining are:

$$X \xrightarrow{RNS} (x_1, x_2, x_3, \dots, x_n) \qquad (2)$$

Where

$$x_i = \langle X \rangle_{m_i}, i = 1,2,3, \dots, n \qquad (3)$$

And $\langle X \rangle_{m_i}$denotes the operation x mod m_i. If the integers X and Y have RNS representations $(x_1, x_2, x_2, \dots, x_n)$ and $(y_1, y_2, y_3, \dots, y_n)$ respectively, then the RNS representation of $Z = XoY$ (where o denotes addition, subtraction, or multiplication) is given by:

$$Z \xrightarrow{RNS} (z_1, z_2, z_3, \dots, z_n) \qquad (4)$$

$$Z_i = \langle x_i o y_i \rangle_{m_i}, i = 1,2,3, \dots, n \qquad (5)$$

What was expressed to up subject understood that arithmetic operations in the RNS executed to parallel, high speed and without any propagation carry. [10,11,12,13,14].

Also for calculate X number of the remainder used of Chinese Remainder Theorem (CRT). This theorem can be expressed as follows:

$$X = \langle \sum_{i=1}^{n} \langle x_i . N_i \rangle_{m_i} \times M_i \rangle_M \qquad (6)$$

Where:

$$M = \prod_{i=1}^{n} m_i \qquad (7)$$

And

$$M_i = \frac{M}{m_i}, N_i = \langle M_i^{-1} \rangle_{m_i}, i = 1,2,3, \dots, n \qquad (8)$$

And the $\langle M_i^{-1} \rangle_{m_i}$ specified in the formula is defined as a multiplicative inverse of M_i modulo m_i [12,13].

In the Residue Number System, executing arithmetic's on the remaining to be done independent and separately. Hence if the one remaining fault occurs its effect on another is not transferred as a result of the inherently RNS architecture is fault tolerant. Therefore the characteristics of the Residue Number System used in applications that are needed to reliability.

III. ONE-HOT RNS

The OHRNS is a method for represents RNS operands using technique one-hot encoding. This technique of encoding allows implementation of arithmetic circuits with lower power consumption and maximum speed. The delay arithmetic operations in this method equal one transistor. Because all major operations like as addition, subtraction, multiplication and modulus conversion are performed using barrel shifters result used of this method is very useful.

For every m_i Moduli remainders are from zero to m_i -1. For m_i moduli remainders are shown in fig. 1that One-Hot representation a signal line is allocated for each of these numbers: The activity of each signal shows the similar remainder with it. In this representation system in each moment only one of the lines are active. By changing the entrance amount, the amount of two lines changes at maximum level. Therefore the power consumption is minimum level.

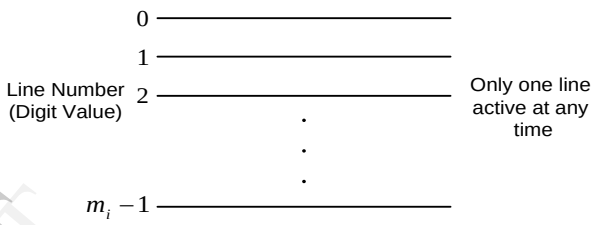
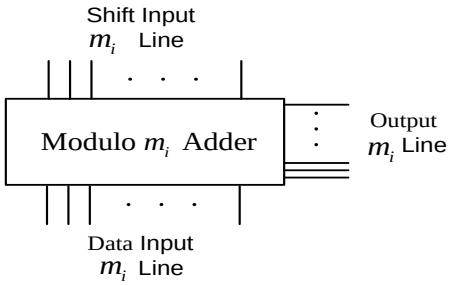


Fig. 1. OHRNS representation for number X_i .

One-Hot Residue Number System is simple and rapid and has regular structure. For implementation one-hot operands, addition is used of a circuit that named barrel shifter. This circuit shift of one operand by an amount equal to the other's value. Barrel shifter, constructed using pass transistors or transmission gates. Which in fig. 2 (a), the two inputs are specified as "shift" and "data" to make the internal operation [fig. 2 (b)] easily understood. The barrel shifter generates, in parallel, all possible rotations of the data input, and selects one of them for output. Which one is selected is determined by the shift input.

The basic hardware in One-Hot is Barrel shifters. In addition to m_i module one of the operands are shifted as the other shifter. The delay of this circuit is equivalent to a transistor.



(a)

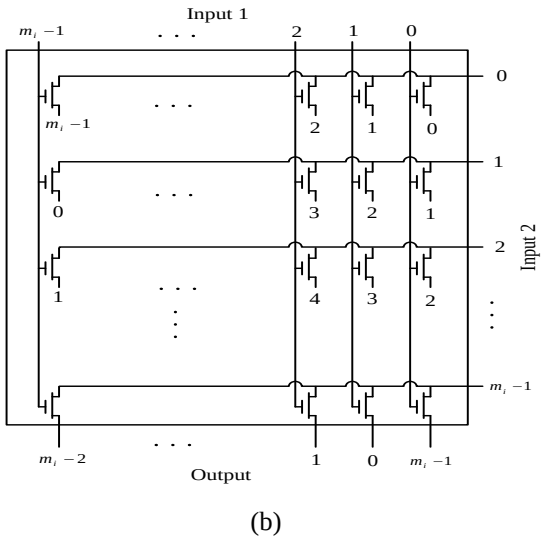


Fig. 2. OHRNS adder: (a) symbol and (b) architecture.

In fig. 3 a one-hot addition is shown for moduli 5 on transistor level. And the transistor delay is shown clearly in this figure. The TG version differs in that it uses transmission gates in place of the pass transistors, and lacks the dual output buffers. Furthermore, the complements of the shift inputs are generated by inverters, one per line, in order to drive the control inputs of the transmission gates.

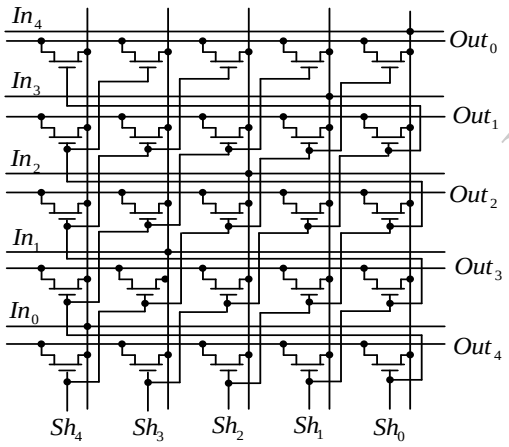


Fig. 3. Modulo 5 OHRNS adder model.

One of the important problems of One-Hot System is that it couldn't be implemented for large moduli since the number of transistor are increased. Main centralization in this paper is rectifying this problem.

IV. Proposed Design for One-Hot Adder/Multiplier

Delay of One-Hot RNS is equal the delay of only one transistor. However, the amount of needed hardware is in the order of m^2, where mis selected module. For example in fig. 4, an adder for module 5 (m=5)is presented. Delay of this adder is equal to delay of one transistor. 25 transistors are needed to compose this circuit.

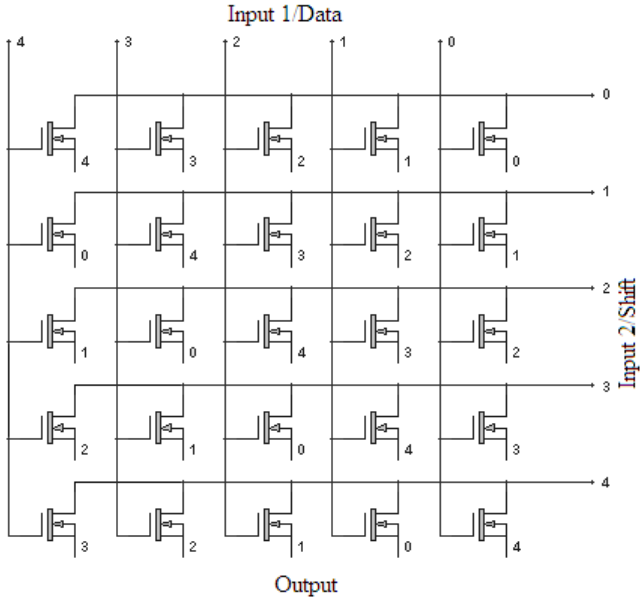


Fig. 4. one hot adder for module 5

Multiply circuit is similar to add circuit with one difference. This difference is order of output to the circuit. In fig. 5, circuit of a multiplier for module 5 is shown.

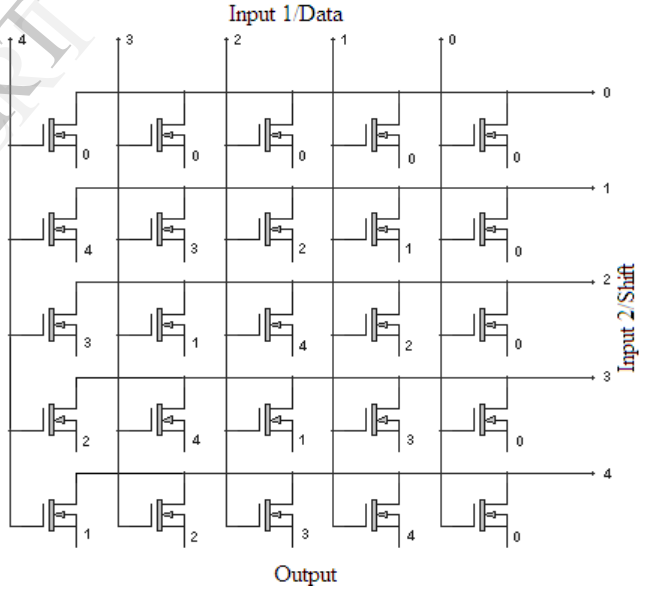


Fig. 5. one hot Multiplier for module 5

As shown in fig. 4 and fig. 5 for every value of input 1 and input 2, only one transistor will be activated. Therefor only one line in output will be activated. For example if line number 2 of input 1 and line number 3 of input 2 are active, only one transistor in adder circuit switched on and line number 0 in adder output will be activated. And in multiplier circuit line number 1 in multiplier output will be activated.

Proposed adder/multiplier circuit for OHR system has two inputs, a and bfor barrel shifter structure, and two outputs, add-outand multiply-out. Each of them has five bits. That is, the module is 5. fig. 6 shows proposed adder/multiplier in OHR for module in special m=5.

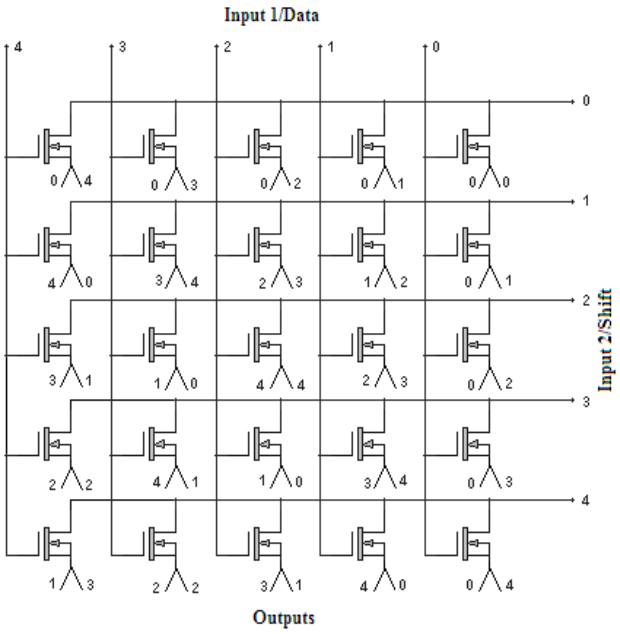


Fig. 6. one hot Adder/Multiplier for module 5

The structure of the proposed one hot Adder/Multiplier can be described as follow.

If line number i (a_i) of input 1 and line number j (b_j) of input 2 are active, only one transistor of proposed circuit switched on. As shown in fig. 7 , if output of active transistor connected to proper line in adder output and multiplier output, only one line of add–out and one line of multiply-out will be activated. Therefor proposed design generates add–out and multiply-out synchronously.

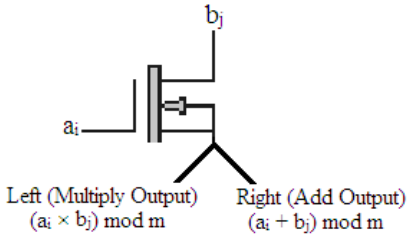


Fig. 7. one transistor of proposed one hot Adder/Multiplier circuit

Proposed design shown in figure 6 present for addition/multiplication operation in module 5. But this method can use for every module 'm' and every operation.

V. COMPARISON

When ever we need both add and multiply operations then we have two barrel shifters. In this case amount of hardware is equal to $2m^2$. And if we need three operations (such as addition, subtraction and multiplication) amount of hardware is equal to $3m^2$. Proposed design one hot adder/multiplier circuit generates both modular add and multiply results. In this design just one barrel Shifter structure is used.

VI. CONCLUSION

Proposed design in this paper generates two operation results (addition and multiplication) synchronously, without change delay, and power consumption in original OHRNS. This design can use for every module and every operation. Proposed method is a MISD and can be used for parallel and pipe line processing.

REFERENCE

[1] W. L. Freking and K. K. Parhi, 1997, "Low-power FIR numberal filters using residue arithmetic," *31st Asilomar Conference on Signals, Systems, and Computers, Pacific Grove, CA, USA*, Vol. 1, pp. 739–43.

[2] P. G. Fernandez, et al.,2000, "A RNS-Based Matrix-Vector-Multiply FCT Architecture for DCT Computation," *Proc. 43rd IEEE Midwest Symposium on Circuits and Systems*, pp. 350-353.

[3] R. Conway and J. Nelson,2004, "Improved RNS FIR Filter Architectures,"*IEEE Transactions On Circuits and Systems II*, Vol. 51, No. 1, pp. 26-28.

[4] A. D. Re, A. Nannareli and M. Re, 2004, "A Tools for Arithmetic Generation of RTL-Level VHDL Description of RNS FIR Filters," *IEEE Proceeding of the Design, Automation and Test in Europe Conference and Exhibition*, pp. 686-687.

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

[6] F. Taylor, 1985, "A Single Modulus ALU for Signal Processing," *IEEE Transactions on Acoustics, Speech, Signal Processing*, Vol. 33, pp. 1302-1315.

[7] J. Ramirez, et al., 2002, "Fast RNS FPL-Based Communications Receiver Design and Implementation," *Proc. 12th Int'l Conf. Field Programmable Logic*, pp. 472-481.

[8] S. Yen, S. Kim, S. Lim and S. Moon, 2003, "RSA Speedup with Chinese Remainder Theorem Immune against Hardware Fault Cryptanalysis," *IEEE Transactions On Computers*, pp. 461-472.

[9] Konoshita E. and lee K., 1997, "A Residue Arichmetic Extension for Reliable Scientific Computation", IEEE Trans. On Computers, Vol. 46, No.2.

[10] A. Chren, Jr., 1998, "One-Hot Residue Coding for Low Delay-Power Product CMOS Design," *IEEE Transactions On Circuits And Systems II: Analog And Numberal Signal Processing*, Vol. 45, No. 3.

[11] A. F. Gonzalez, and P. Mazumdar, Redundant Arithmetic, 2000, "Algorithms and Implementations," *Integration: The VLSI Journal*, Vol. 30, No. 1, pp. 13-53.

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

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

[14] S. Hanzawa, T. Sakata, K. Kajigaya, R. Takemura, and T. Kawahara, 2005, "A Large-Scale and Low-Power CAM Architecture Featuring a One-Hot-Spot Block Code for IP-Address Lookup in a Network Router," *IEEE Journal of Solid-State Circuits*, Vol. 40, No. 4.