International Mathematical Forum, 5, 2010, no. 59, 2911 - 2918

An Optimum Moduli Set in Residue Number System

Somayyeh Jafarali Jassbi[1]

Islamic Azad University Science and Research branch, Tehran, Iran
sjasbi@sr.iau.ac.ir

Keivan Navi

Department of Electrical and Computer Engineering
Shahid Beheshti University, Tehran, Iran
navi@sbu.ac.ir

Ahmad Khademzadeh

Iran Telecommunication Research Center, Tehran, Iran
zadeh@itrc.ac.ir

Abstract

The Residue Number System (RNS) is an unconventional system. This system is a useful tool for Digital Signal Processing (DSP) since it can support parallel, carry-free, high-speed, low power and secure arithmetic. One of the most important things we should consider for RNS is the choice of the moduli set. It should cover the system's speed, its dynamic range, as well as its hardware complexity depends on both the forms and the number of the chosen moduli.
In this paper an optimum moduli set
$\{3^n-1,3^n+1,3^n+2,3^n-2\}$ is illustrated.
Comparisons demonstrate that we have achieved a significant improvement in terms of speed.

Keywords: Residue Number System, Multi-Level Residue Number System, One-Hot Residue Number system, Multiple-Valued Logic.

[1] Corresponding author: Somayyeh Jafarali Jassbi, E-mailsjasbi@sr.iau.ac.ir

1- Residue Number System

Residue Number System is unconventional and non- Weighted Number System in which the additions, subtractions and multiplication are inherently carry free.
As a result we may add, subtract and multiply numbers in one step regardless of the length of the number involved. An integer X is represented in the Residue Number System by an n-tuple $(x_1, x_2, ..., x_n)$ where x_i is a nonnegative integer satisfy $X = m_i q_i + r_i$. This causes an increase in calculation speed and a reduction in its power consumption.
Residue Number System is specified by moduli set like $(m_1, m_2, ..., m_n)$ in which all the moduli are positive integers. If all the moduli are relatively pair wise prime the system will have the largest possible dynamic range which equals $[\alpha, \alpha + M)$ in which α is an integer and M is:

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

The integer X in $\alpha \le X < \alpha + M$ has a single representation in Residue Number System which is shown by the set of remainders $(x_1, x_2, x_3, \dots, x_n)$. In this way:

$$x_i = X \mod m_i \quad , i = 1, 2, \dots n$$

In order to reconstructing the specified number X the remainders $(x_1, x_2, x_3, \dots, x_n)$ the Chinese Remainder Theorem is applied as follows:

$$X = \left\langle \sum_{i=1}^{n} (x_i N_i)_{m_i} \times M_i \right\rangle_M \text{ , 1 , 1, 2,3, ,}$$

$$M = \prod_{i=1}^{n} M_i$$

$$M_i = \frac{M}{m_i} \quad , N_i = \left\langle M_i^{-1} \right\rangle_{m_i} , i = 1, 2, 3, \dots, n$$

In which $\left\langle M_i^{-1} \right\rangle_{m_i}$ is defined as multiplicative inverse M_i with m_i moduli [8].

Due to its special features, the Residue Number System has many applications in arithmetic functions such as Digital Signal Processing, Digital Filtering, Coding, RSA ciphering system, digital communications, Ad-hoc network, storing and retrieving information, Error detection and Correction, and fault tolerant systems. This system is generally used in those areas where addition, subtraction and multiplication operations of numbers are being repeated. Moreover, since in this system the calculations on the remainders are done independently if one error occurs on one remainder it won't be transferred to other moduli. In other words, the architecture of RNS is inherently tolerant against faults and error detection and correction are quite possible [5- 12].
In the second, third and forth chapters of this article, Multi- Level Residue Number System , Ternary Valued Logic and One-Hot Residue Number System will be examined respectively. In chapter five an optimum Moduli Set $\{3^n - 1, 3^n + 1, 3^n + 2, 3^n - 2\}$ in Residue Number System is represented. In chapter six

New Moduli Set will be compared to other moduli Set. Finally an overall conclusion will be represented.

2- Multi-Level RNS

Considering the impact of Residue Number System in increasing calculation speed, reducing power consumption, and increasing the security and fault tolerance, it would be possible to perform arithmetic calculations on each modulus with a new Residue Number System. It is possible to repeat this procedure until we reach very small moduli, in other words this procedure could be repeated in several levels. The system which is achieved form the above mentioned procedure is called Multi-Level Residue Number System. The only restriction that should be considered in Multi-Level Residue is that the Residue Number System dynamic range that is considered for i level of each (i-1) moduli-level should be greater or equal to those moduli[3-8].
In this article, for having a more simple representation two-level Residue Number System is being analyzed. It should be mentioned that this method could be generalized to more than two levels.
In two-level Residue Number System, two symmetrical coding key algorithms are used inside each other.
Therefore the system has a much higher security level than the Residue Number System. The other advantage of two-level Residue Systems is the simple selection of moduli set for a large dynamic range that is by selecting a few large moduli and applying a new Residue Number System with a lower power for second level this capability is achieved. By having few moduli with higher power in the first level; first the need for moduli to be relatively pair wise prime is eliminated and there is no obligation for the moduli to be symmetric and regular, second as the number of moduli is reduced the concerning conversion circuits, become simple and the operation is done rapidly. Also, in the second level since the moduli are small because of the limited propagation of carries, the internal calculations of the Residue Number System are done faster.

3- Ternary Valued Logic

Despite binary logic in which logical levels are restricted to two possible states, namely false and true, there exists an alternative named Multiple Valued Logic.
In this system, theoretically, one can define an unlimited number of logical levels, but in reality it is limited and this limitation mainly depends on the used technology. In Ternary valued logic with 3 levels comprising {0,1, 2} , we can introduce a new era.
It is obvious that the positional weights of any two succeeding columns are power of 3. Figure 1 represents the positional value of each location.

$$a_{n-1}\,a_{n-2}\,a_{n-3}\ldots a_2\,a_1\,a$$
$$---------$$
$$3^{n-1}\,3^{n-2}\;\;3^{n-3}\ldots 3^2\,3^1\,3^0$$

Fig. 1. Positional weight value of each location

Each location in an TVL component can store much more information than a binary logic component can, the dynamic range of the moduli set $\{3^n-2,3^n-1,3^n\}$ is much greater than its equivalent in the binary representation. Now the question is how to present the related hardware which is clearly answered in [7-9].
For example if we compare two different moduli sets with equal number of locations, the results illustrated in Table 1 will be obtained.

Table 1. Comparison of dynamic range and number of location

Moduli Set	Number Of Position	M
$\{3^n-2,3^n-1,3^n\}$	3n	$3^{3n}-2^{2n+1}+2'$ 3^n
$\{2^n-1,2^n,2^{n-1}-1\}$	3n	$2^{3n-1}-1.5(2^{2n})+2$
$\{2^n-1,2^n,2^n+1\}$	3n+1	$2^{3n}-2^n$

Table 2. Comparison of dynamic with different n.

n / M	5	10
$3^{3n}-2^{2n+1}+2'\;\;3^n$	14172246	$@2'$ 10^{14}
$2^{3n-1}-1.5(2^{2n})+2^n$	14880	$@5'$ 10^8
$2^{3n}-2^n$	32736	$@10^9$

Based on these comparisons, we conclude that the TVL with the same number of locations has a much larger dynamic range.

4-One-Hot Residue Number System

In the One-Hot residue number system we discuss in m_i that is the reminder of moduli .they are shown from zero to $m_i - 1$ .in One-Hot we define a signal line dedicated for each reminder. in this system it is rule that in each moment only one of the lines is on and active.its structure is so simple with high speed and so the power consumption is low. the function of this system is base on barrel shifter that has shift entry and data entry.in addition to m_i moduli one of the operand are shifted as the other shifter. [8,14, 13, 16]

This system can use for small moduli, but we should consider that it cannot be implemented for larg moduli [8, 14].

One–Hot representation for m_i moduli remainders are shown in figure 2 [14].

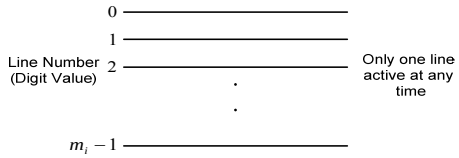


Figure 2 – One-Hot representation for m_i re mainders.

In figure 3 [14] this operation is represented for moduli 4 by a graph.

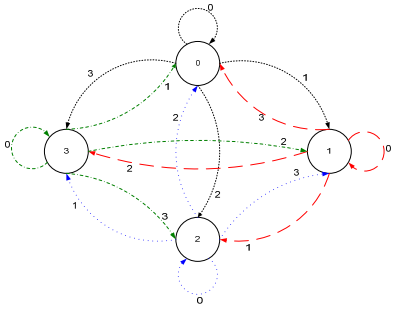
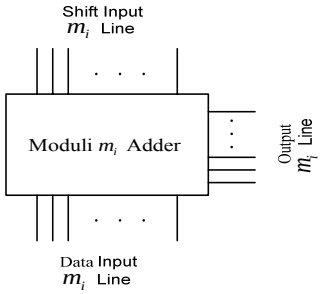


Figure 3 – Addition Position for Moduli 4

In this figure we have a graph that all of operand has relation to each other on the base of reminders. In One-Hot residue number system our delay reduced to one transistor.

As we mentioned the main element in One-Hot is Barrel shifters. In figure 4A represented two entries: data entry and shift entry, and in figure 4B is One-Hot addition is represented [14].



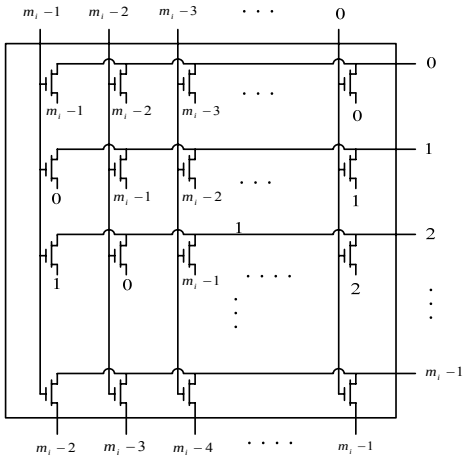


Figure 4-A- Additive symbol of On-Hot for m_i moduli

Figure 4-B- Additive symbol of On-Hot for m_i moduli

One of the short comings of One-Hot System is that it couldn't be implemented for large moduli since the number of transistor are increased. Therefore this system is suitable for small moduli but practically it is not applicable for large moduli.

5- An Optimum Moduli Set

$$\{3^n-1,3^n+1,3^n+2,3^n-2\}$$

In this paper One-Hot Multi-Level moduli set $\{3^n-1,3^n+1,3^n+2,3^n-2\}$ in ternary logic is presented. In first level the moduli set $\{3^{2n}-1,3^{2n}-4\}$ is used this moduli are relatively prime. Then for the second level the moduli set $\{\{3^n-1,3^n+1\},\{3^n+2,3^n-2\}\}$ is considered for $\{3^{2n}-1,3^{2n}-4\}$ For RNS conversion, first we convert to the first level and then we convert the remainder of first level to the second level. In order to do the reverse conversion we do the same job but from bottom to up. Which means, first we convert the second level to the first level and then we convert the remainder of first level to weighted number system.

Then we use One-Hot to reduce the number of transistors. Now with this system the delay become low and the speed become so faster and therefore the power consumption become very low.

6- Conclusion

In this paper Two-Level RNS, two symmetrical key encryption algorithms are used together, so the system has a high security. Another advantage of Two-Level RNS is the simple selection moduli set for large dynamic range. So comparisons demonstrate that we have achieved a significant improvement in terms of speed because we combine One-Hot Residue Number system.

References

[1]A. Skavantzos and M. Abdallah, "Implementation Issues of the Two-Level Residue Number System
with Pairs of Conjugate Moduli," *IEEE Transactions On Signal Processing*, Vol. 47, No. 3, Mar. 1999.

[2] H. Krishna, K.-Y. Lin, and J.-D. Sun, "A coding theory approach to error control in redundant Residue Number Systems - Part I: theory and single error correction," *IEEE Trans. Circuits Syst.*, Vol. 39, pp. 8-17, Jan. 1992.

[3] H. M. Yassine, "Hierachical Residue Number System suitable for VLSI Arithmetic Architectures"
IEEE International Symposium on Circuits and Systems, Vol. 2, pp. 811-814, May 1992.

[4] J.-D. Sun and H. Krishna, "A coding theory approach to error control in redundant Residue
Number Systems -Part II: multiple error detection and correction," *IEEE Trans. Circuits Syst*., Vol.39, pp. 18-34, Jan. 1992.

[5] Jean-Claude Bajard, Laurent Imbert, "A Full Implementation RSA in RNS," *IEEE Transactions on Computer*, Vol. 53, No.6, Jun. 2004.

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

[7] M. Abdallah and A. Skavantzos, "On Multi Moduli Residue Number Systems With Moduli of Forms {r a ,r b - 1,r c + 1} ," *IEEE Transactions Circuits System I: Regular Paper*, Vol. 52, No. 7, pp. 1253- 1266, 2005.

[8] M. Hosseinzadeh, S. J. Jassbi and K. Navi, "A Novel Multiple Valued Logic OHRNS Moduli r^n Adder Circuit," *International Conference on ENGINEERING AND TECHNOLOGY,* Vol. 25, pp. 128-132, Nov. 2007.

[9] M. Hosseinzadeh, K. Navi, S. Gorgin, "A New Moduli Set for RNS: $\{r^n - 2, r^n - 1, r^n\}$,"
International Conference on Electrical Engineering 2007, Apr. 11-12, 2007.

[10] M. Hosseinzadeh and K. Navi, "A New Moduli Set for Residue Number System in Ternary Valued
Logic," *Journal of Applied Sciences*, Vol. 7, No. 23, pp. 3729-3735, 2007.

[11] N. S. Szabo and R. I. Tanaka, "Residue Arithmetic and Its Applications to Computer Technology," New York :McGraw-Hill, 1967.

[12] Parhami B., "RNS Representation with Redundant Residues," *Proc. of the 35th Asilomar Conference on Signals, Systems, and Computers*, Pacific Grove, CA, pp. 1651-1655, Nov. 2001.

[13] S. Hanzawa, T. Sakata, K. Kajigaya, R. Takemura, and T. Kawahara, "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, Apr. 2005.

[14] S. Jafarali Jassbi, M.Hosseinzadeh, S.Gorgin, K.Navi,"One-Hot Multi-Level Residue Number System"5th IEEE East-West Design and Test International Symposium, Yerevan, sept.2007.

[15] S. Timarchi, K. Navi and M. Hosseinzadeh, "New Design of RNS Subtractor for modulo $(2n+1)$," *2th IEEE International Conference on Information & Communication Technologies: From Theory To Applications*, Apr. 2006.

[16] W. A. Chren., "Delta–Sigma Modulator with Large OSR Using the One-Hot Residue Number System," IEEE Transactions on Circuits and Systems—II: Analog and Digital Signal Processing, Vol. 46, No. 8, Aug. 1999.

Received: July, 2010