International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 05 Issue: 03 | Mar-2018 www.irjet.net p-ISSN: 2395-0072

Implementation of FIR Filter using Self Tested 2^n-2^k-1 Modulo Adder

B.Soujanya[1], P.Koteswara Rao[2]

[1]Pursuing M.Tech & Universal College of Engineering & Technology
[2]Assistant Professor, Dept. of ECE, Universal College of Engineering & Technology, AP, India.

Abstract - *Modulo adder is one of the key components for the application of residue number system (RNS). Moduli set with the form of 2^n-2^k-1 can offer excellent balance among the RNS channels for multi-channels RNS processing. In this project, a novel algorithm and its VLSI implementation structure are proposed for modulo adder. In the proposed algorithm, parallel prefix operation and carry correction techniques are adopted to eliminate the re-computation of carries. Any existing parallel prefix structure can be used in the proposed structure. Thus, we can get flexible trade-off between area and delay with the proposed structure. Compared with same type modulo adder with traditional structures, the proposed modulo adder offers better performance in delay and area. In this project the proposed adder is used to generate random numbers which are repeated after a long period which can be useful for cryptographic applications. And also the proposed modulo adder is self-tested by making use of Linear Feedback Shift Register (LFSR). Using the same modulo adder, an FIR filter is implemented and compared with the general FIR filter to prove the better performance of Residue Number System to the normal computation.*

Key Words: **Modulo Adder, Random Number Generator, Finite Impulse Response Filter, Linear Feedback Shift Register, Delay.**

1. INTRODUCTION

Random numbers have been in use for thousands of years. During ancient times random numbers were generated by using dice, coins, playing cards, and many other techniques. Even today, random numbers play an important role as it is used in cryptographic operations. For example it is used for generating keys in both symmetric and asymmetric algorithms, encryption, masking protocols...etc [1].Random number generator is an algorithm, which, based on an initial seed, produces a sequence of numbers. The main requirement is that this sequence should appear random to any observer. Random number generator may be software based or hardware-based systems [2], [3]. Hardware-based systems for random number generation are widely used. Various methods to compute pseudo-random numbers are known [4]. Most of them are based, on linear congruential equations [5] and require a number of time consuming arithmetic operations. In contrast, the use of feedback shift registers permits very fast generation of binary sequences. Shift register sequences of maximum length (m-sequences) are well suited to simulate truly random binary Sequences.

In this project, Random number generator is constructed by using modulo $2^n - 2^k - 1$ adder for residue number system. According to the form of the modulus, modular adders can be classified into two types: the general modular adder and the special modular adder.

In 1987, Magdy A Bayoumi suggested a method for arbitrary modulus in which the binary adders are cascaded [6]. There are many other literatures on implementing modular adders using two parallel binary adders that calculate A+B and A+B+T [7], [8]. Even though the delay is small it requires about twice area of binary adder.

In 1992 Dugdale proposed a method to construct a type of general modular adders that uses same adder for both A+B and A+B+T addition [9]. The main drawback of this structure is that it requires two operation cycles to perform one modular addition.

In 2002 Hiasat proposed a class of modular adders in which the final stage is constructed by using Carry Look Ahead (CLA) based binary adder [10]. But this structure requires an extra CLA unit to obtain the carry-out bit of A+B+T. As a result, the structure does not reduce the delay significantly.

In 2004 Patel et al [11] proposed ELMMA algorithm. which uses one carry computation module for A+B and other carry computation module for A+B+T in which some carry computation units can be shared.

In 2008 S. H. Lin and M. H. Sheu proposed an architecture for modulo 2^{n+1} [12] adder based on "diminished-1" number representation. But this structure has more delay. A similar architecture for modulo 2^n+3 [13] adder was proposed by, P. M. Matutino, R. Chaves, and L. Sousa in 2010.

The random number generator using modulo $2^n - 2^k - 1$ adder [14] consists of four units, the pre-processing, the carry generation, the carry modification and the sum calculation module. A new class of general modular adder with better performance in delay can be constructed by using the proposed modular adder. In the proposed scheme, the carries of A+B+T is computed first. These carries are modified twice to obtain the final carries

required in the sum computation module. Meanwhile, in the proposed modular adder structure any existing fast prefix structure of binary adders can be used, which offers flexibility in the design.

2. BACKGROUND

2.1. Residue Number System

A residue number system is defined by a set of moduli, which consists of n pair wise relatively prime integers $\{m_0, m_1, m_2...,m_{n-1}\}$. The total count of numbers that can be represented by this number system is called range. It is the proc $\prod_{i=0}^{n-1}$ i in the moduli set.

$$M=\prod_{i=0} m_i \qquad (1)$$

Such a residue number system is able to uniquely represent unsigned numbers in the range [0,M -1] and signed numbers in the range [-(M-1)/2 ,((M+1)/2)-1] for odd values of M, or [-M/2,(M/2)-1] for even values of M. These are called the dynamic range of the system. A number Y within the dynamic range is represented by its residues y_i with respect to the moduli m_i. The representation of Y in RNS is denoted as

$$Y = \{y_0, y_1, y_2...,y_{n-1}\} \qquad (2)$$

Where $i = 0,1,...,n-1$. In RNS addition, subtraction and multiplication can be performed entirely on the residue representation of the operands. Let the RNS representations of

$$X = \{x_0, x_1, x_2...,x_{m-1}\} \text{ and}$$
$$Y = \{y_0, y_1, y_2...,y_{m-1}\} \text{ and}$$

$$|X \text{ o } Y| = \{| x_0 \text{ o } y_0|m_0, |x_1 \text{ o } y_1|m_1 ,..., |x_{n-1} \text{ o } y_{n-1}|m_{n-1}\} \quad (3)$$

where the operation 'o' can be either addition or subtraction or multiplication. Note that the arithmetic operation o is performed in parallel with no interaction between the RNS channels. As a result the RNS systems are capable of performing high-speed addition and multiplication compared to traditional two's complement systems.

2.2. Residue Addition

For n-bit moduli m, where $m < 2^n$, $n = [\log_2 m]$ and where [c] represents the smallest integer greater than c, we formulate the modular addition problem as

$$C=(A+B)_m=\begin{cases} A+B & A+B<m \\ A+B-m & A+B\geq m \end{cases} \qquad (4)$$

where A, B and C are all n-bit unsigned integers. The subtraction in the above equation can be replaced by an addition of the additive inverse of m mod 2^n, t (=2^n-m)[8] and, as a result, the modular addition equation above can be redefined as

$$C=(A+B)_m=\begin{cases} A+B & A+B+T<2^n \\ A+B-m & A+B+T\geq 2^n \end{cases} \qquad (5)$$

The equation for C above identifies the general approach used to perform modular addition. If the carry from the binary sum A+B + T is 1 then the output of the modular addition is the n least significant bits (LSBs) of the resulting sum. Otherwise, the result is n-bit sum of A+B.

3. MODULO $2^N - 2^K - 1$ ADDER

The modulo adder is composed of four modules, pre-processing module, carry generation module, carry modification module, and sum calculation module. In Figure 1, different shade represents different processing modules. The modulo $2^n - 2^k - 1$ adder can be divided into two general binary adders, A1 and A2, with carry modification and sum calculation module according to the characteristics of correction T. We can get the carries $c_i$real used in the final stage through correcting the carries c_iT of A+B+T which can be computed by any existing prefix structure with proper pre- processing. At last, we can get the final modular addition result from c_i real and partial sum information. The proposed architecture shown in Fig. 2 can avoid the calculation of carries information for and separately. Thus, the area and delay in VLSI implementation can be reduced.

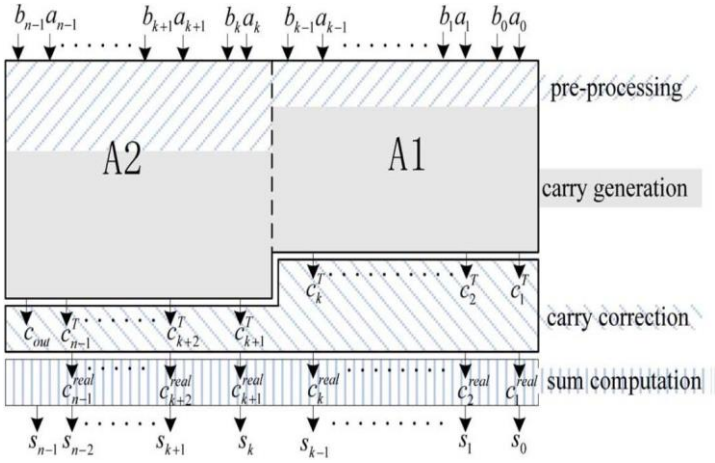
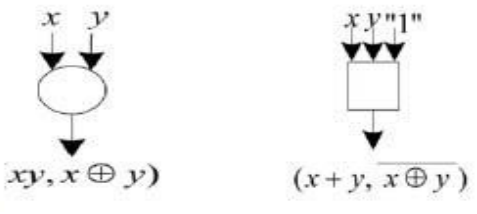


Figure 1: $2^n - 2^k - 1$ Modulo Adder used in Proposed FIR filter

3.1 Preprocessing unit

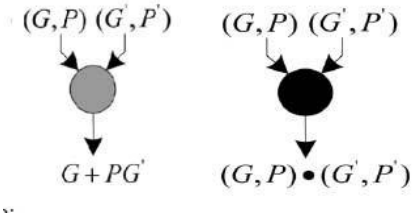
The purpose of pre-processing unit is to generate the carry generation and propagation bits (gi,pi) of A+B+T. The computation of A+B+T is performed by A1 and A2

where A1 and A2 are used for lower-k bits and higher (n-k) bits addition respectively. Two modules Preprocessing A1 and preprocessing A2 are taken. The functions white square and white circle are used in this module.



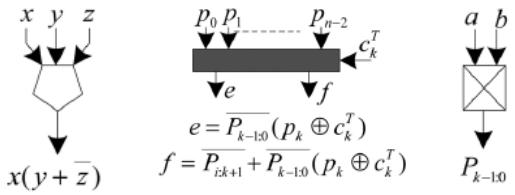
3.2 Carry generation unit

Generation and carry propagation bits from the pre-processing unit are used to get the carries of A+B+T. Any existing prefix structure can be used to get the carries. Here sklansky prefix adder is used. Two modules Prefix computation A1 and Prefix computation A2 are taken. The functions used in this module are Gray circle and black circle.



3.3 Carry modification unit

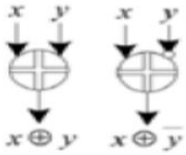
The carry modification unit is used to get the real carries for each bit needed in the final sum calculation stage. In order to reduce the area, we get the carries of A+B by correcting the carries of A+B+T in the carry correction unit. Twice carry correction is done for both adders A1 and A2 to generate real carries.



3.4 Sum calculation unit

In this unit, the partial sum bits from both A+B and A+B+T are required . Two functions are used in this module; Inverse XOR circle and XOR circle. The sum bits are

$$s_i = \begin{cases} \overline{c_{out}} \oplus p_0 & i=0 \\ c^k_{real} \oplus \overline{c_{out}} \oplus p_k & i=k \\ c^i_{real} \oplus p_i & i=1,\ldots,k-1,\ldots,n-1 \end{cases} \quad (6)$$



The resulting structure is shown in the Fig.2

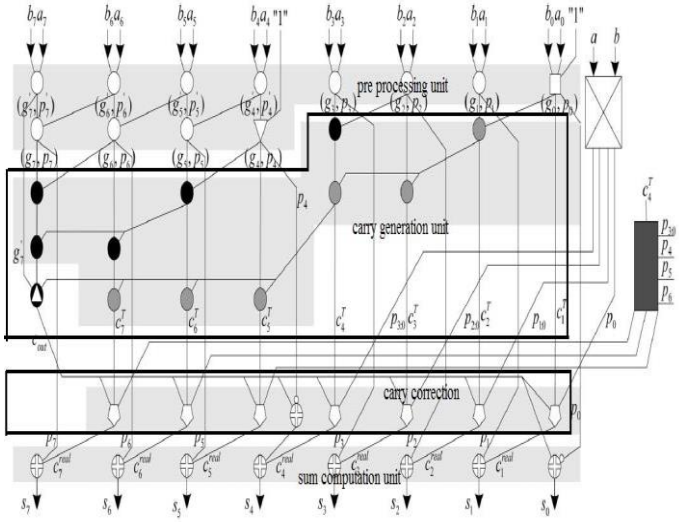


Figure 2: The modulo $2^8 - 2^4 - 1$ adder

3.5 Generation of Random Number

Random number generator is an algorithm that, based on an initial seed, produces a sequence of numbers. The main requirement is that this sequence appears random to any observer. Here, in this paper we are generating random numbers using modulo $2^n - 2^k - 1$ adder and LFSR (Linear feedback shift register) in which modular adder has large dynamic range and better performance. A large value of m(modulo) is desired, so that the period can be kept long in which random numbers can be generated that are secure for cryptographic applications .In this paper a random number generator is constructed with a period of $2^{11*8} - 1$.

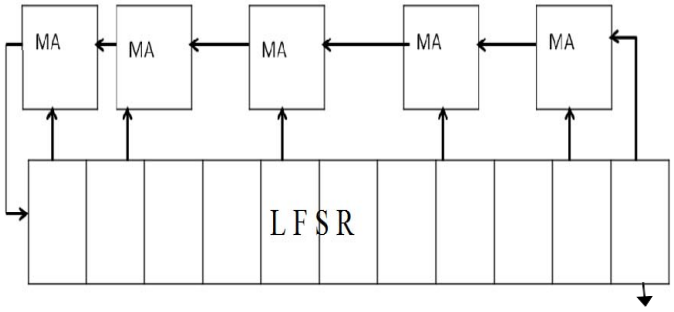


Figure 3: Random Number Generation with self Testing

4. EXISTING & PROPOSED SYSTEMS

The Conventional FIR filter is the existing system with general adder for adding filter coefficients. Consider the Causal FIR filter whose equation is given by

$$y[n] = b_0x[n] + b_1x[n-1] + \cdots + b_Nx[n-N] = \sum_{i=0}^{N} b_i \cdot x[n-i], \quad (7)$$

The following is the existing FIR system with Novel General Adder

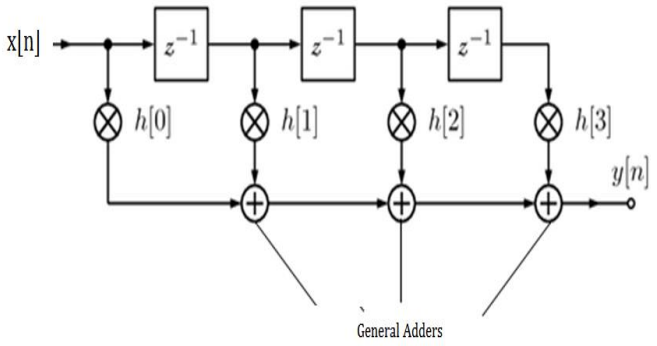


Figure 4: Conventional FIR Filter

In Proposed system, we are replacing the general adder by a modulo adder which is discussed in this paper in figure1.The proposed system is shown in below figure.

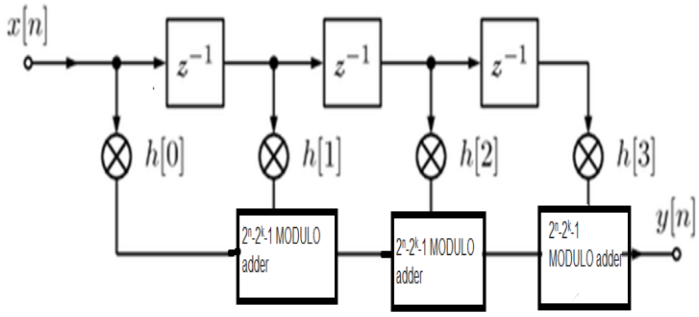


Figure 5: Proposed FIR Filter with Modulo Adder

From the synthesis reports of both the filters, it is observed that modulo $2^n - 2^k - 1$ adder has a delay of 11.21ns which is much better and faster than that of conventional filter 26.69ns. The number of registers used is 12, which is also less than the conventional filter. This shows that the area required by the modulo $2^n - 2^k - 1$ adder is less than the other.

The following table gives you the delay values in detail

Table-1: Comparison of Results

Type	Delay	Number of registers
Conventional FIR filter	26.69 ns	44
FIR filter with modulo adder	11.21 ns	12

5. Simulation Results

The simulation results are performed in Xilinx software, Synthesis reports were generated. Synthesis reports give the details about Delay of the proposed and existing FIR Filters

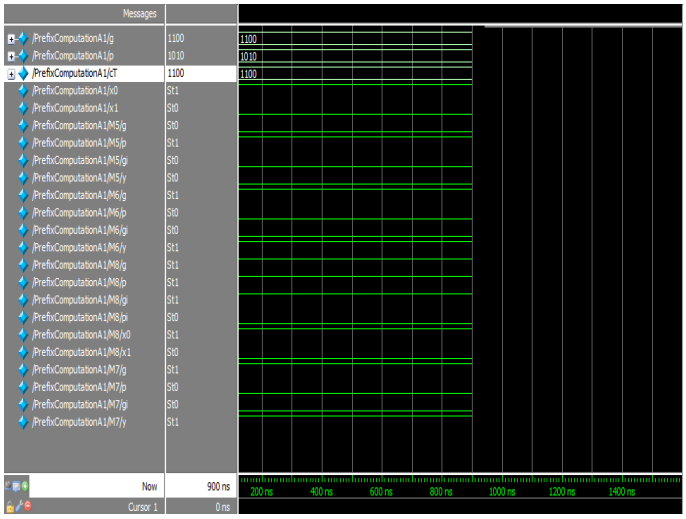


Figure 6: Simulation result for pre-processing unit

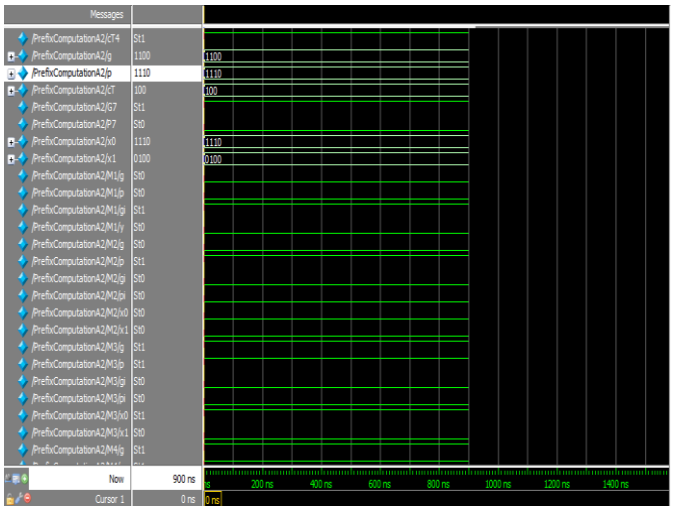


Figure 7: Simulation result for prefix computation

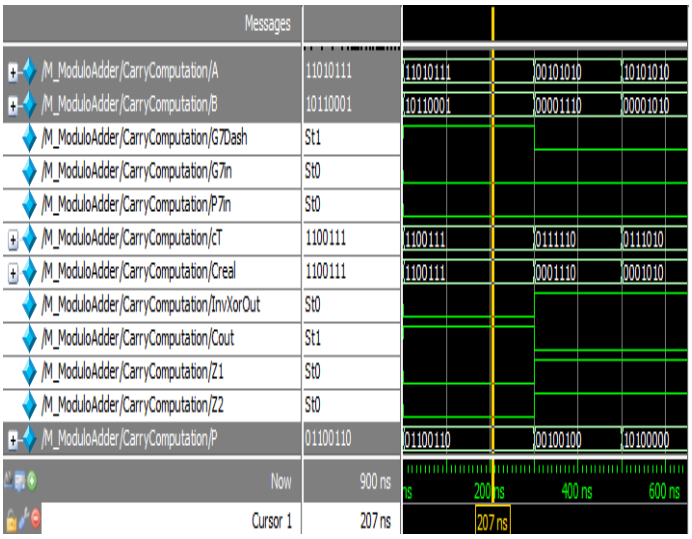


Figure 8: Carry Computation Block simulation result

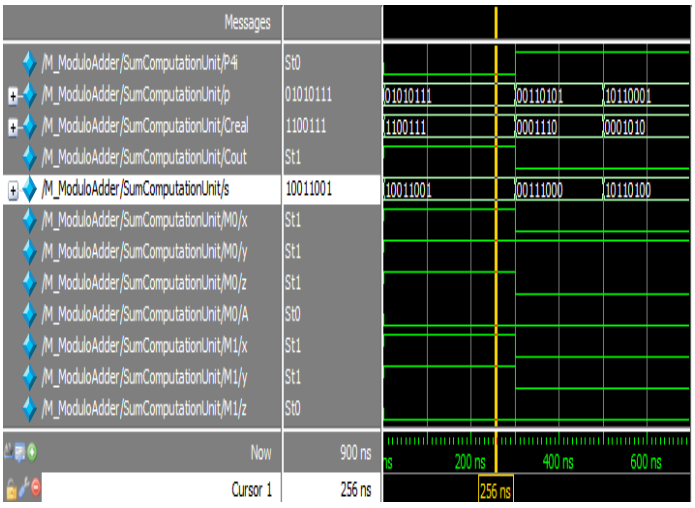


Figure 9: Sum Computation simulation result

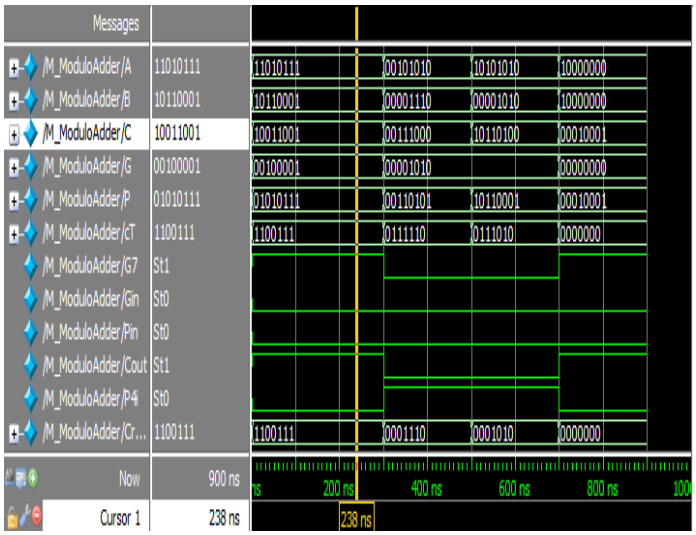


Figure 10: Modulo Adder Output simulation Result.

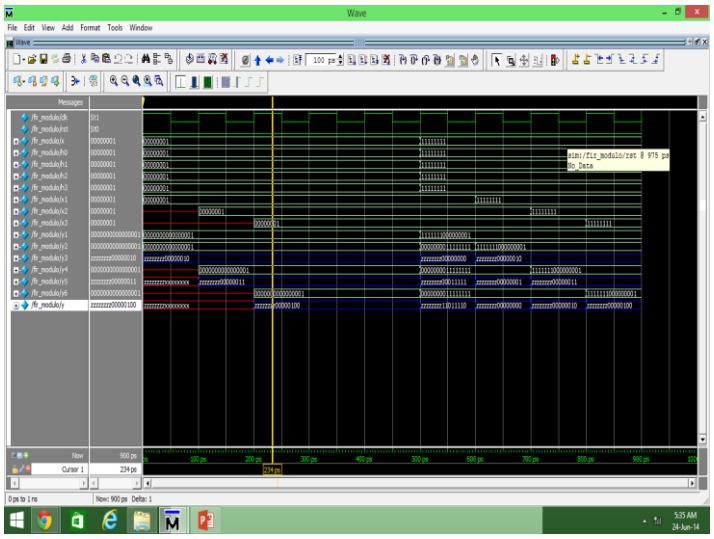


Figure 11: Simulation result for FIR filter using modulo adder

6. CONCLUSION

In this paper , a new FIR Filter with modulo 2^n-2^k-1 adder is proposed. Using this adder random numbers are generated with high dynamic range .This structure consists of pre-processing unit, carry generation unit, carry correction unit and sum computation unit. The way using twice carry correction improves the performance of area and timing. This modulo adder has given better performance in area and delay compared to general modulo adder. Implementation of efficient FIR filter using modulo 2^n-2^k-1 is done with a delay of 11ns. By comparing this with conventional FIR filter, it has given high speed and is efficient.

REFERENCES

[1] Data Conversion in Residue Number System, Omar Abdelfattah, Department of Electrical & Computer Engineering McGill University Montreal, Canada ,January 2011

[2] A good tutorial paper of RNS: Fred J. Taylor, "Residue Arithmetic: A Tutorial with Examples", IEEE Trans. on Computer, pp. 50~62, May 1994.

[3] A good paper collections for RNS: M. A. Soderstrand, W. K. Jenkins, G. A. Jullien, F. J. Taylor (eds.), Residue Number System Arithmetic: Modern Applications in digital Signal Processing, IEEE Press, New York, 1991.

[4] On Modulo 2^n + 1 Adder Design, Haridimos T. Vergos, Member, IEEE, and Giorgos Dimitrakopoulos, Member, IEEE,IEEE TRANSACTIONS ON COMPUTERS, VOL. 61, NO. 2, FEBRUARY 2012.

[5] Low Power Realization of Residue Number System based FIR Filters, M. N. Mahesh, Mahesh Mehendale Texas Instruments (INDIA) Ltd.

[6] A Novel Low Complexity Combinational RNS Multiplier Using Parallel Prefix AdderMohammad R. Reshadinezhad, Farshad Kabiri Samani, IJCSI International Journal of Computer Science Issues, Vol. 10, Issue 2, No 3, March 2013.

[7] Computer Arithmetic Circuits ∗ Lecture 9: Residue Number SystemsFebruary 2006.

[8] RNS-To-Binary Converter for a New Three-Moduli Set 2^{n+1}- 1; 2^n; 2^n- 1Pemmaraju V. Ananda Mohan, Fellow, IEEE