RANDOM NUMBER GENERATION USING MODULO 2N-2K-1 ADDER FOR RESIDUE NUMBER SYSTEM

P.Mamatha¹, D.Chandra Mohan², Dr.M.Gurunadha babu

Abstract: Modulo adder is the vital component in the Residue number system. In this paper modulo 2n-2k-1 adder is proposed to generate random numbers for use in cryptographic applications. Moduli set with the form of 2n-2k-1 (1≤k≤n-2) is the best suitable for multi-channel RNS processing [1]. In this proposed algorithm twice carry correction technique is used and thus it reduces area and delay compared with same type modulo adder with traditional structures [1]. This algorithm is developed in Xilinx 14.2 using Verilog HDL.

Keywords - Cryptography, random numbers, RNS, twice carry correction.

I. INTRODUCTION
Residue number system, in contrast with decimal and binary number system is a non-weighted and non-positional system. This number system works on finite ring and moduli of the system. For RNS which has carry-free property, there are two operations: addition and multiplication. For integers X and Y with n-bit width, modular addition can be performed by

\[ Z = [X + Y]_m = \begin{cases} \frac{X + Y}{m} & \text{if } X + Y < m \\ \frac{X + Y}{m} - m & \text{if } X + Y \geq m \end{cases} \]

Where T is the carry correction and m is the modulus.

II. RELATED WORK
This paper explains the generation of random numbers using the novel modulo 2n-2k-1 adder to show the better performance compared to standard adders. Also, the same modulo adder can also be used for self-testing using the Linear Feedback Shift Registers (LFSR).

III. MODULO 2N-2K-1 ADDER
This proposed modulo adder is divided into two general binary adders, A1 and A2 with carry correction and sum computation modules.

<table>
<thead>
<tr>
<th>TABLE 1: MODULES</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pre-processing Unit</td>
</tr>
<tr>
<td>Adder A1</td>
</tr>
<tr>
<td>Prefix computation unit</td>
</tr>
<tr>
<td>Carry correction unit</td>
</tr>
<tr>
<td>Sum Computation unit</td>
</tr>
</tbody>
</table>

Example:
Consider
\[ X=(a7,a6,a5,a4,a3,a2,a1,a0) = (1,1,0,1,0,1,1,1) \]
\[ Y=(b7,b6,b5,b4,b3,b2,b1,b0) = (1,0,1,0,0,0,1) \]
Then \[ g[7:0]=0,0,1,0,0,0,1,1 \]
\[ p[7:0]=0,1,0,1,1,1,10 \]

1. PRE-PROCESSING UNIT
The purpose of pre-processing unit is to generate the carry generation and propagation bits (gi,pi) of X+Y+T. The computation of X+Y+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 the preprocessing modules.
The function used in this module are Gray circle and black circle are used.

\[ (G, P) \quad (G, P') \]
\[ G + PG' \quad (G, P') \]

Example:
Considering the above gi and pi bits
\[ C[6:0]=(1,1,0,0,1,1,1) \]
And Cout=1

3. CARRY CORRECTION UNIT
The carry correction unit is used to get the real carries for each bit needed in the final sum computation stage. In order to reduce the area, we get the carries of \( X+Y \) by correcting the carries of \( X+Y+T \) in the carry correction unit. Twice carry correction is done for both adders A1 and A2 to generate real carries.

Three functions are used in this module: white pentagon, cross square and black box.

Example: \[ c_{\text{real}}[7:1]=(1,1,1,1,0,0,1,1) \]

4. SUM COMPUTATION
In this unit, the partial sum bits from both \( X+Y \) and \( X+Y+T \) are required.

Two functions are used in this module; Inverse XOR circle and XOR circle.

Example:
Considering the above values we get the sum as
\[ \text{Sum}[7:0]=(1,0,0,1,1,0,0,1) \]
Which is binary equivalent of 153.

5. PROPOSED MODULO ADDER

IV. GENERATION OF RANDOM NUMBERS

A random number generator is a computational or physical device designed to generate a sequence of number that lack any pattern i.e. appear random. Here, in this paper we are generating random numbers using this modulo adder which has large dynamic range and better performance.

As a large value of \( m(\text{modulo}) \) is desired, so that the period can be kept long in which random numbers can be generated that are secure for cryptographic applications.
V. SIMULATION RESULTS

![Simulation result for modulo adder](image1)

![Simulation result for random number generation](image2)

VI. CONCLUSION

In this paper modulo $2^n \cdot 2^{k-1}$ adder is implemented and using this random numbers are generated that can be repeated after a long period which is secure for cryptographic applications. The way using twice carry corrections improves the performance of area and timing in VLSI implementation and reduces the redundant units for parallel computation of $X+Y+T$ and in the traditional modular adders.

VII. ACKNOWLEDGEMENTS

This work is carried out based on the paper entitled “A Novel Modulo $2^n \cdot 2^{k-1}$ Adder for Residue Number System”. We would like to express our sincere gratitude and thanks to authors named Shang Ma, Jian-Hao Hu, and Chen-Hao Wang for having motivated us to take up the problem of modulo $2^n \cdot 2^{k-1}$ adder.

REFERENCES

Journal Papers:
[1]. A novel modulo $2^n \cdot 2^{k-1}$ adder for residue number by Shang Ma, Jian-Hao Hu, Member, IEEE, and Chen-Hao Wang ieeetransactionsoncircuitsandsystems—i:regularpapers-2013


[3]. 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

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


Books:

Theses:
[7]. Omar Abdelftah. Data conversion in Residue number system McGill University, Montreal, Canada, in M.E 2011.