VLSI HARDWARE MODELING OF DYNAMIC RNS STRUCTURE FOR HIGHEND COMPUTATIONS

GANJI SARIKA YADAV¹, V.THRIMURTHULU², S.ALI ASGAR³
¹²³ Department of Electronics and Communication Engineering
¹ II M.TECH (VLSISD), CR Engineering College, Tirupati, Chittoor (Dist), A.P., India.
² Professor & HOD., Dept. of ECE, CR Engineering College, Tirupati, Chittoor (Dist), A.P., INDIA.
³ Assistant Professor, Dept. of ECE, CR Engineering College, Tirupati, Chittoor (Dist), A.P., INDIA.
¹ ganjisarika@gmail.com, ² vtmurthy.v@gmail.com, ³ aliasgarsvyed@gmail.com

ABSTRACT
This paper presents a dynamic structure for binary-to-residue number system (RNS) conversion modulo \( \{2^n \pm k\} \) using macro structures. This structure is based only on adders and constant multipliers. This concise work is motivated by the existing \( \{2^n \pm k\} \) binary-to-RNS converters, which are particular inefficient for larger values of \( n \). The experimental results obtained for 8 X n bits of dynamic range suggest that the projected conversion structures are able to drastically progress the forward conversion efficiency, with greater successful hardware modelling. And macro modelling can highly increase proper selection and utilization of the \( \{2^n \pm k\} \) Moduli for high end applications like Cryptography. The proposed logistic technique is simulated and verified by Xilinx tools along with Virtex – 5 FPGA board.

Index Terms — RNS, Macro Modeling, cryptography, Xilinx tools and Virtex -5 FPGA.

1. INTRODUCTION
It is very familiar that the Residue Number System (RNS) has modular nature by means with offers the prospective for swift, parallel reckoning since that it is a carry-free calculation system, also it is to be noted that RNS is a non-weighted number system, which uses remainders to represent numbers [1]. The basic arithmetic operations (add, subtract, and multiply) are easily implemented in RNS and data computations are implemented over operands that are extensively shorter than the resulting RNS Dynamic Range. Typical applications for RNS are in VLSI Digital Signal Processing (DSP), Cryptography, Network Security, High end filtering, convolutions, correlations, and Fast Fourier Transform computations [2]-[3] etc. Basically the RNS modulus set is set up by defining the moduli of (m₁) relatively positive prime integers. A number \( P \) is represented in RNS by its residues \( p_i = \langle X m_i \rangle \), where \( p_i \) is the remainder of the division of \( X \) by \( m_i \), and then to implement complete RNS system Conversion from weighted number system to RNS (binary to-RNS or forward conversion), and vice versa (RNS-to-binary or reverse conversion) is required. At the very beginning the development of proposed system on RNS was mainly persistent on the three modulus set \( \{2^n - 1, 2^n, 2^n + 1\} \)[4], but today the research has been extended to dynamic range of prime integers also such as \( \{2^n - k, 2^n, 2^n + k\} \)[3]-[5], \( k \in Z^+ \) such that the implementation of such method can drastically improves the circuit performance.

The literature survey reveals the fact that various techniques are already proposed [6] like serial method, full parallel method or serial-parallel technique etc, to reduce the weight representation of the number systems, which is the root cause of occupying lot of system memory and consumes unwanted power consumption and finally the architectures for high end process applications becomes much more slower. Therefore a new memory-less standard [7] forward conversion structure for a DR of \( m = qn \)-bit, using \( \{2^n \pm k\} \) moduli, is proposed, considering \( n \geq 2 \). The projected approach divides the \( qn \) input bits into \( q \) input sets[8], and computes the particular residue value using modular additions and constant multiplications[9] so that the idea of constant multipliers does not lead to any excess memory consumption[10].

A. DESIGN DEVELOPMENT
To promote low power high performance applications of RNS, Various dynamic macro techniques are modeled on VLSI. The VLSI architectures developed as follows. The VLSI architecture proposed with this article for use of RNS is to reduce on chip memory consumption adopts the macro selection condition which results in to dynamic implementation of major techniques. All these techniques are modeled and implemented by targeting the area and power consumption, the next proceeding section will conclude all about proposed scheme. This proposal is also realized into field programmable gate array (FPGA) prototyping system using Xilinx Virtex-5 unit. The maximum operating frequency of this design is more than 500 MHz.
2. MODELING OF RNS TECHNIQUES

B. RNS Representation:
An RNS is defined by a set of relatively prime integers called the moduli. The moduli-set is denoted as \{m_1, m_2, \ldots, m_n\} where \(m_i\) is the \(i^{th}\) modulus. Each integer can be represented as a set of smaller integers called the residues. The residue-set is denoted as \{r_1, r_2, \ldots, r_n\} where \(r_i\) is the \(i^{th}\) residue. The residue \(r_i\) is defined as the least positive remainder when \(X\) is divided by the modulus. This relation can be symbolically written based on the congruence: \(X \equiv r_i \mod m_i\). The same congruence can be written in an alternative notation as \(\lfloor X / m_i \rfloor \mod r_i\). The RNS is capable of uniquely representing all integers that lie in its dynamic range. The dynamic range \(\{m_1, m_2, \ldots, m_n\}\) is determined by the moduli-set and denoted as

\[
M = \prod_{i=1}^{n} m_i
\]  

(1)

The RNS provides exceptional depiction for all integers in the range between 0 and \(N\), where \(N\) is the full dynamic range, it is required to compute in order to attain the residue modulo \(\{2^n - 1\}\) of \(X\).

\[
\langle X \rangle_{2^n - k} = \left(2^{3n} X_{[4n-1:3n]} + 2^{2n} X_{[3n-1:2n]} + 2^n X_{[2n-1:n]} + X_{[n-1:0]}\right)_{2^n - k}
\]

\[
= \left(2^{3n} X_3 + 2^{2n} X_2 + 2^n X_1 + X_0\right)_{2^n - k}
\]

\[
= \left(k^3 X_3 + k^2 X_2 + kX_1 + X_0\right)_{2^n - K}
\]

Where \(X_{[k: l]}\) represents the bits \(l\) to \(k\) of the integer \(X\).

Similarly, the residue calculation modulo \(\{2^n + k\}\), is achieved as

\[
\langle X \rangle_{2^n + k} = \left(2^{3n} X_{[4n-1:3n]} + 2^{2n} X_{[3n-1:2n]} + 2^n X_{[2n-1:n]} + X_{[n-1:0]}\right)_{2^n + k}
\]

\[
= \left(2^{3n} X_3 + 2^{2n} X_2 + 2^n X_1 + X_0\right)_{2^n + k}
\]

\[
= \left(-k^3 X_3 + k^2 X_2 - kX_1 + X_0\right)_{2^n + K}
\]

(2)

Taking into deliberation the meticulous cases of modulo \(\{2^n - 1\}\) and \(\{2^n + 1\}\), conversion from binary-to-RNS can be performed as per given calculation.

\[
\langle X \rangle_{2^{n-1}} = \left(N_3 + N_2 + N_1 + N_0\right)_{2^{n-1}}
\]

\[
\langle X \rangle_{2^{n+1}} = \left(-N_3 + N_2 - N_1 + N_0\right)_{2^{n+1}}
\]

(4)

(5)

Proposed architecture for modulo \(\{2^n \pm k\}\) presumptuous conversion is based on a parallel technique. In this technique partial operation \((k, X_i)\) is first condensed to modulo \(\{2^n \pm k\}\), and only then added to obtain the final residue value. Thus, computation is performed in two stages: the first step computes the constant multiplication

---

**TABLE 1 SUMMARY OF DESIGN CONSIDERATIONS**

<table>
<thead>
<tr>
<th>S.No</th>
<th>Design consideration</th>
<th>Selection</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Compiler</td>
<td>Xilinx14.4Vivado</td>
</tr>
<tr>
<td>2</td>
<td>Programming Language</td>
<td>Verilog</td>
</tr>
<tr>
<td>3</td>
<td>FPGA</td>
<td>Virtex -5</td>
</tr>
<tr>
<td>4</td>
<td>Interface</td>
<td>USB</td>
</tr>
</tbody>
</table>

**C. Mathematical Modelling of RNS conversion:**

Allowing for a binary representation of \(X\), with \(4n\)-bit of Dynamic Range, it is required to compute in order to attain the residue modulo \(\{2^n - k\}\) of \(X\).
vectors and the second step performs the addition of all those vectors. This architecture exhibits the modular reduction of each calculation, using the modulo \(2^n \pm k\) Carry-Save-Adder, instead of adding all terms and reducing then iteratively at the conclusion. The suggested architecture is as shown below.

![Architecture of RNS](image)

The key design of this architecture that the macros are associated in the design description which facilitates the logic transfer from one stage to other for example one bit length to other bit length can be easily avail without changing the complete architecture. The implementation of macros lead to this proposed system works in various bit lengths as 8, 16, 32 and 64.

**D. Front-End Modeling:**
This phase of implementation contains the following stages simulation using Xilinx 14.4 Vivado suite, synthesis using Xilinx 14.4 XST and verifying on Virtex – 5 FPGA board.

**3. SIMULATION AND SYNTHESIS RESULTS**
The Verilog RTL Description of the above article is simulated and synthesized using Xilinx14.4 (ISE-Simulator), implementation of all the above macro encoding techniques are successfully synthesized and verified on Virtex - 5 FPGA board and the results are shown below.

![Simulation output for n = 8](image)

![Synthesis output for n = 8](image)

![Simulation output for n = 16](image)

![Synthesis output for n = 16](image)
CONCLUSION
In this paper, we have presented VLSI hardware modelling of macro level implementation set of RNS designed at reducing the power dissipated by the weighted representation of traditional technique of number systems used in high end applications. In addition, their part is usual to increase in potential technology of memory usage. This paper has realized with Xilinx tools along with Virtex -5 FPGA. Such designs are suggested to exhibits a competitive performance with current work.

ACKNOWLEDGMENT
I express my sincere thanks to my guide and Project Coordinator Mr.S.ALI ASGAR, M.Tech. Assistant Professor of ECE Dept, and to my HEAD OF DEPARTMENT Dr.V.THRIMURTHULU.
REFERENCES


AUTHORS

Ganji Sarika Yadav received her B.Tech degree in Electronics & Communication Engineering from SV Engineering College for Women, Tirupati (A.P), India, in the year 2013. Currently pursuing her M.Tech degree in VLSI System Design at Chadalawada Ramanamma Engineering College, Tirupati (A.P), India. Her area of research includes low power VLSI design.

Dr. V. Thrimurthulu, M.E., Ph.D., MIETE, MISTE. Professor & Head of ECE Dept. He received his Graduation in Electronics & Communication Engineering AMIETE in 1994 from Institute of Electronics & Telecommunication Engineering, New Delhi, Post Graduation in Engineering M.E specialization in Microwaves and Radar Engineering in the year Feb, 2003, from University College of Engineering, Osmania University, Hyderabad, and his Doctorate in philosophy Ph.D from central University, in the year 2012. He has done his research work on Ad-Hoc Networks.

S. Ali Asgar was born in Tirupati, Andhra Pradesh, India. He received B.Tech degree in Electronics and Instrumentation engineering from Sree Vidyanikethan engineering college, A.Rangampet in the year 2007. He did his M. Tech. in Digital Signals in 2012 from SJ CET, yemmiganur (A.P), India. He is currently working as Associate Professor in Chadalawada Ramanamma Engineering College, Tirupati (A.P), and India.