Effective Moduli, Superior RNS: The Strategic use of Conjugate Sets

G Appala Naidu
Assistant Professor, JNTU-GV College of Engineering, Vizianagaram, India

Abstract. The System which uses Residue Number System need to deliberately select moduli set, so that it is more useful in forward conversion and reverse conversion for the better Performance. In this paper, Conjugate moduli set $\{2^{n_1}-1, 2^{n_1}+1, 2^{n_2}-1, 2^{n_2}+1, 2^{n_3}-1, 2^{n_3}+1, \ldots\ldots\ldots 2^{n_L}-1, 2^{n_L}+1\}$ **proposed to use in forward conversion and reverse conversion methods to obtain optimized area and delay values. For verifying the results, the software tool used is Xilinx 14.7 ISE with Virtex-7 FPGA kit and the targeted device xc7vx330t-3ffg1157. The proposed Conjugate moduli set based Forward Conversion and Reverse Conversion compared with the different moduli sets available in the literature and corresponding codes written in Verilog HDL code, compiled, simulated with the help of ISIM Simulator. After this, it is Synthesized for utilization summary. From the performance comparison, Proposed moduli set in forward conversion contributed area 26.32% increased and delay 19.19% decreased and on the other side i.e. in reverse conversion methods, CRT had the improvement in area 62.03% and in delay 30.73%, MRC had the improvement in area 13.41% and in delay worse performance by -24.02%, New CRT-I had the improvement in area 23.52% and in delay 22.73%, New CRT-II had the improvement in area 18.71% and in delay 27.23%. These obtained results can be useful in applications like DSP Signal processing applications, Radar Signal processing applications.**

Keywords: Residue Number System (RNS), Forward Conversion, Reverse Conversion, Conjugate moduli set.

I. INTRODUCTION

The efficiency, power consumption, area, and latency of electronic systems are critical factors for both current and future platforms, particularly for portable devices [1], [2]. In order to satisfy these demands, parallelism can be used at multiple levels of electronic system design, including a variety of architectures and algorithms that allow arithmetic calculations to be performed concurrently on smaller components. This strategy supports lower power consumption and enhanced computational performance [3]. However, conventional weighted binary number systems remain limited by extended carry-propagation paths, which lead to higher latency and inefficient power utilization. These challenges have accelerated research into alternative number representations, particularly the Residue Number System (RNS) [4,5].Unlike traditional weighted systems, RNS enables arithmetic operations i.e. except division [22]where each digit is processed independently, eliminating carry propagation. This characteristic substantially improves throughput and energy efficiency, making RNS especially attractive for digital signal processing (DSP) applications. Additionally, the independence of modulo channels in RNS contributes to improved fault tolerance. Consequently, RNS has been adopted in cryptographic systems including RSA [6,7], fault-tolerant architectures, FLP-based communication receivers [8], DSP [9,24], digital image processing (DIP) [10], RADAR signal processing [11,23], and other high-performance computing applications [12,13].

1.1 Residue Number System

The Residue Number System (RNS) has emerged as an important resource as in [14], in the field of digital arithmetic, providing benefits in terms of computational efficiency and parallelism. It's effective RNS design requires diligent consideration of essential factors such as moduli set choice, forward and reverse conversion, and residue arithmetic unit design in [12]. Each of these components influences the performance and effectiveness of RNS-based computations.

- **Moduli set selection** is a critical aspect of RNS design, as it determines the system's dynamic range and computational efficiency. Selecting an appropriate set of pairwise coprime moduli is essential to support wide numerical ranges in practical applications [12], [15].

- **Forward conversion** transforms a weighted binary number into its residue representation by computing remainders with respect to each modulus [15], [16]. Efficient conversion techniques improve accuracy and arithmetic performance within RNS architectures [17], [19].
- **Residue arithmetic units**, consisting of modular adders, subtractors, and multipliers, operate independently across modulo channels, reducing complexity and enabling high-performance computation [15].
- **Reverse conversion** reconstructs the weighted binary number from residues using methods such as the Chinese Remainder Theorem (CRT), Mixed Radix Conversion (MRC), and New CRT-I/II, ensuring compatibility with conventional systems [15], [16], [18], [20]. Addressing these core design aspects enables efficient and practical RNS-based computational systems [19].

RNS representation: An RNS is determined by the moduli, a collection of comparatively prime integers. The moduli-set is abbreviated as $\{m_1, m_2, m_3, m_4, m_5, \ldots\ldots m_n\}$with "$m_i$" denoting the i[th] modulus. Each integer can be thought of as a collection of smaller integers, referred to as residues. The label for the residue set reads $\{r_1, r_2, r_3, r_4, r_5, \ldots\ldots r_n\}$,where "$r_i$" stands for the i[th] modulus. The residue r_i is known as the smallest positive residue when divided by the modulus m_i. When divided by the modulus mi, the residue r_i is defined as the least positive remainder as in [21]. On the basis of congruence, this relationship can be written in the following manner:

$$X \bmod m_i = r_i \quad (1)$$

In an alternate notation, the same coherence can be written as:

$$|X|_{m_i} = r_i \quad (2)$$

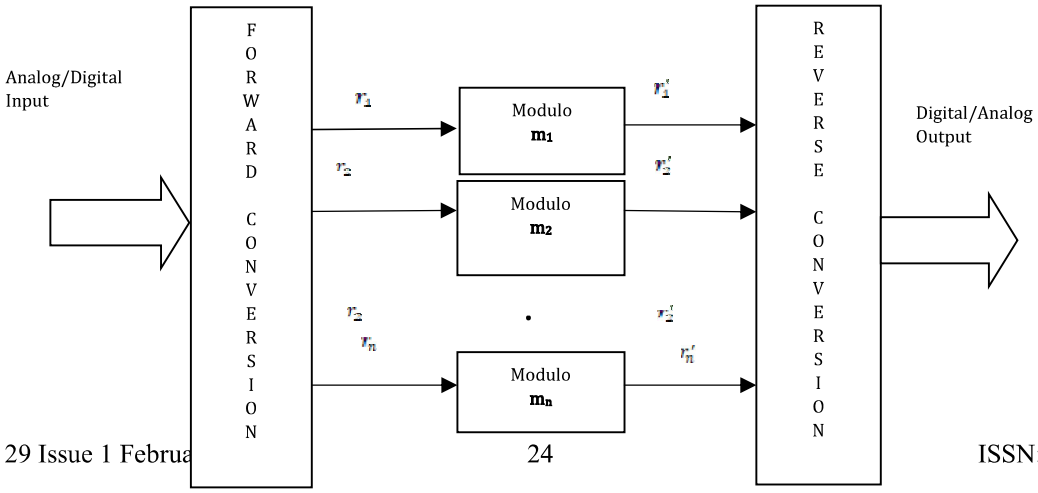
Both integers X which residue in its dynamic spectrum can be uniquely constituted by the RNS. The product of moduli-set $\{m_1, m_2, m_3, m_4, m_5, \ldots\ldots m_n\}$ defines the dynamic range and denotes it as M,

$$M = \prod_{i=1}^{n} m_i \quad (3)$$

The RNS provides specific representations for all numbers in the range 0 to M-1. If the integer X is bigger than M-1, same representation will repeat.

In RNS, residue representations repeat, causing multiple integers to share identical residue sets; therefore, the moduli must be pairwise coprime to fully utilize the maximum dynamic range M. The weighted binary input is converted into residues using a forward converter, after which arithmetic operations such as addition, subtraction, and multiplication are performed in parallel without carry propagation, enabling high-speed computation [19]. Each modulus is associated with an independent arithmetic unit comprising modular adders, subtractors, and multipliers. The computed residues are then transformed back into weighted binary form using a reverse converter. A typical RNS architecture, illustrated in Fig. 1, consists of three main blocks: forward conversion, residue arithmetic unit, and reverse conversion.

Fig. 1. Typical RNS System block diagram



Year	Moduli Sets		Decimal Input	Residue Sets Output
[28]	$\{2^n-1, 2^n, 2^n+1, 2^{2n}+1\}$	{3,4,5,17}	718	{1,2,3,4}
[29]	$\{2^n-1, 2^n, 2^n+1, 2^{n+1}-1\}$	{3,4,5,7}	298	{1,2,3,4}
[29]	$\{2^n-1, 2^n, 2^n+1, 2^{n+1}+1\}$	{7,8,9,17}	2010	{1,2,3,4}
[30]	$\{2^n-3, 2^n+1, 2^n-1, 2^n+3\}$	{5,9,7,11}	1676	{1,2,3,4}
[31]	$\{2^n-1, 2^n+1, 2^{2n}-2, 2^{2n+1}-3\}$	{3,5,14,29}	787	{1,2,3,4}
[32]	$\{2^n-1, 2^n, 2^n+1, 2^{2n+1}-1\}$	{3,4,5,31}	1678	{1,2,3,4}
[32]	$\{2^n-1, 2^n+1, 2^{2n}, 2^{2n}+1\}$	{3,5,16,17}	2707	{1,2,3,4}
[33]	$\{2^n+1, 2^n-1, 2^n, 2^{n+1}+1\}$	{9,7,8,17}	667	{1,2,3,4}
[34]	$\{2^n, 2^{n+1}-1, 2^n-1, 2^{n-1}-1\}$	{16,31,15,7}	7473	{1,2,3,4}
[35]	$\{2^{n_1}-2, 2^{n_1}+2, 2^{n_2}-2, 2^{n_2}+2\}$	{6,10,14,18}	1890	{1,2,3,4}
[36]	$\{2^n, 2^{n-1}-1, 2^n-1, 2^{n+1}-1\}$	{16,7,15,31}	5553	{1,2,3,4}
[37]	$\{2^{n-1}, 2^n-1, 2^n+1, 2^{2n+1}-1\}$	{2,3,5,31}	593	{1,2,3,4}
[38]	$\{2^{n-1}, 2^n-1, 2^{n-1}-1, 2^{n+1}-1\}$	{8,15,7,31}	5057	{1,2,3,4}
[39]	$\{2^{4n}, 2^{2n}+1, 2^n+1, 2^n-1\}$	{256,17,5,3}	56833	{1,2,3,4}
[40]	$\{2^{n-1}, 2^n-1, 2^{n-1}-1, 2^{n+1}-1\}$	{15,17,31,33}	5087	{1,2,3,4}
Proposed	$\{2^{n_1}-1, 2^{n_1}+1, 2^{n_2}-1, 2^{n_2}+1\}$	{7,3,31,11}	4250	{1,2,3,4}

Table 1. Moduli sets, Decimal inputs and Residue sets

The forward conversion maps the input data into an RNS representation, while the reverse conversion restores the RNS output to a conventional form. These stages significantly influence the overall efficiency of an RNS system, as the complexity and delay of the conversion circuitry can offset the speed benefits of RNS processing. Interfacing with the analog domain typically involves an intermediate binary conversion stage, which increases the latency and the complexity. To enable an RNS processor to compete with a binary-based DSP system [27], efficient conversion techniques are required. The reverse conversion commonly employs the Chinese Remainder Theorem (CRT) and the Mixed-Radix Conversion (MRC) methods, while ongoing research on direct analog-to-residue (A/R) and residue-to-analog (R/A) converters aims to eliminate the intermediate stage and improve the overall performance.

II. LITERATURE REVIEW

The efficient implementation of Residue Number System (RNS) design is dependent on numerous essential elements, including moduli set selection, forward conversion, residue arithmetic units, and reverse conversion. The choice of moduli has a considerable impact on the system's dynamic range, speed, and hardware complexity. RNS provides a wide range of moduli sets essential for system optimization. The forward converter efficiently converts weighted binary numbers to their RNS form utilizing independent converters for each modulus and multi-operand modular adders. The reverse converter, on the other hand, aims to decrease conversion time while increasing area efficiency, making it essential for advanced RNS activities such as division and magnitude comparison.

Cao et al. [28] proposed an efficient reverse converter for the 4-moduli set

$\{2^n - 1, 2^n, 2^n + 1, 2^{2n} + 1\}$using the new Chinese Remainder Theorem (CRT). This novel solution takes advantage of the moduli set's unique qualities to execute modulo repairs without using expensive and time-consuming modulo operations. The architecture is simplified to include simply bit reorientation and a multioperand modular adder, which increases both area and time complexity. The proposed converter showed higher efficiency, with an area complexity equivalent to 4n full adders (FAs) and a delay of approximately 2n FAs for the high-speed (HS) version, and an area complexity of 3n FAs and a delay of about 2.5n FAs for the cost-effective (CE) version. These results show significant gains over other 4-moduli sets, indicating that the suggested design is more efficient in terms of hardware space and computing delay.

Mohan et al. [29] provided efficient designs for Residue Number System (RNS) to binary converters utilizing two novel four-module sets: $\{2^n - 1, 2^n, 2^n + 1, 2^{n+1} - 1\}$and $\{2^n - 1, 2^n, 2^n + 1, 2^{n+1} + 1\}$.These designs use the Mixed-Radix Conversion (MRC) method in a multi-level architecture to increase speed while decreasing hardware complexity. Mohammad Obeidi Daghlavi et al. [30] proposed efficient two-level reverse converters to handle the four-moduli set, using New Chinese Remainder Theorem I (New CRT-I) and Mixed Radix Conversion, that include ROM-free and adder-based structures for VLSI circuits, accomplishing significant performance improvements in Area-Time (AT) metrics, about FPGA implementations exhibiting a 12%-10% enhancement over current designs, thereby rendering them highly efficient for high-speed arithmetic applications. which increases both area and time complexity. The proposed converter showed higher efficiency, with an area complexity equivalent to 4n full adders (FAs) and a delay of approximately 2n FAs for the high-speed (HS) version, and an area complexity of 3n FAs and a delay of about 2.5n FAs for the cost-effective (CE) version. These results show significant gains over other 4-moduli sets. This research collectively helps to improve the efficiency and effectiveness of RNS and forward & reverse converter designs. However, more research is required to address implementation issues, maximize performance across multiple moduli sets, and investigate power consumption and scalability. Choosing feasible moduli sets is critical for improving performance and efficiency in RNS systems. From the literature survey conducted in previous and from the above research papers, the following moduli sets taken for discussion in this research paper and same taken for performance comparison. These complete moduli set information for discussion shown in Table 1., it consists of reference year, moduli set used or proposed in that paper, for different values of ‘n’, decimal input, based on moduli set considered and decimal input the resultant residue set. In addition to these moduli sets, at last proposed conjugate moduli set also shown for reference.

The purpose of this research is to improve the efficiency and efficacy of RNS designs. Despite previous advances, more study is required to address implementation difficulties, maximize performance across different moduli sets, and investigate power consumption and scalability. The proper selection of moduli sets is critical to increasing RNS system performance and efficiency. Using our literature survey, we found and compared distinct moduli sets. The residue arithmetic unit operates on these sets. These findings have significant effects for applications like as signal processing, RADAR signal processing, and cryptography.

III. METHODOLOGY

The performance of a Residue Number System (RNS) design is significantly affected by the moduli set used. The RNS system's efficiency and effectiveness are significantly affected by the moduli set used. According to literature, careful evaluation of moduli is critical for improving system performance, making it an important aspect in RNS-based solutions. Conjugate moduli, in particular, have a significant impact on RNS design performance. Adding conjugate moduli pairs to a two-level RNS can dramatically increase the system's efficiency and functionality. This approach improves accuracy while lowering computing costs, making it a key element in RNS design.

The proposed approach provides an effective method for optimizing area and delay requirements. By employing a two-stage architecture that integrates forward and reverse conversion with advanced techniques such as a conjugate moduli set and New Chinese Remainder Theorems (CRTs), the system achieves higher computational efficiency, reduced complexity, and faster processing speed. Prior work by Skavantzos and Abdallah demonstrates that this approach not only optimizes RNS designs but also enables compact hardware implementations, significantly reducing area and system delay.The proposed forward conversion scheme using conjugate moduli combines theoretical insights with hardware-efficient design to improve speed and efficiency. It merges a Mod $2^{n_1} - 1$and a Mod $2^{n_1} + 1$stage into a single Mod $2^{2n_1} - 1$unit, and similarly combines Mod $2^{n_2} - 1$and

Mod $2^{n_2}+1$into a Mod $2^{2n_2}-1$unit. This integration enhances performance while reducing hardware overhead. The resulting architecture offers an efficient and scalable solution for RNS forward conversion, with applications in digital signal processing and cryptography. Fig. 2 illustrates the proposed forward conversion block diagram.

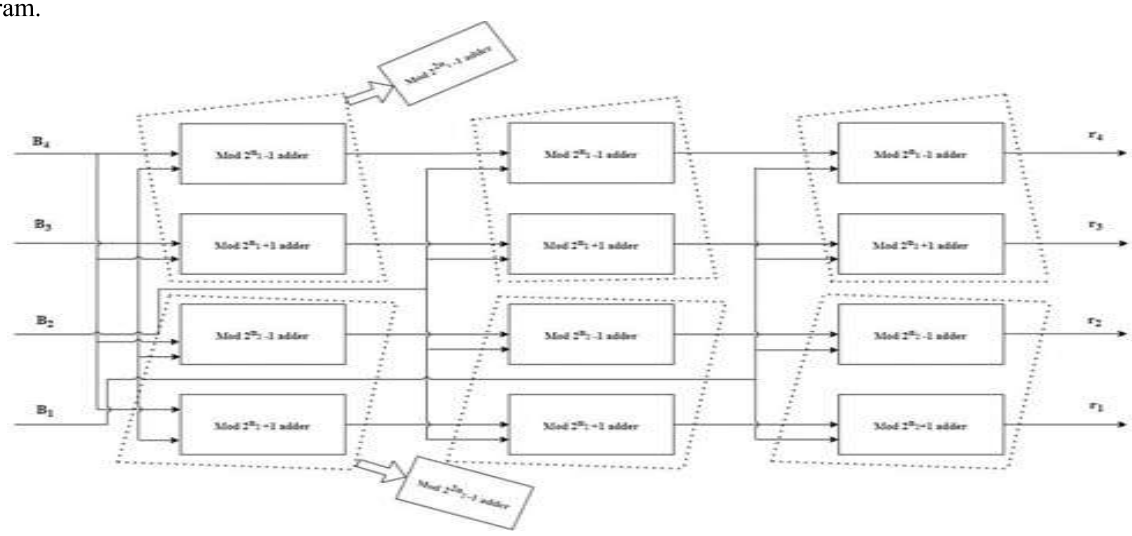
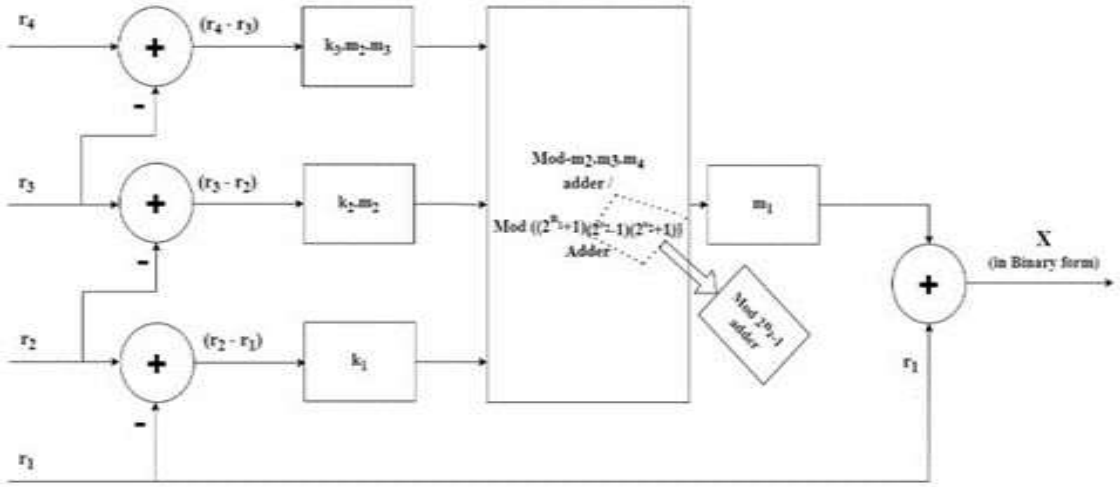
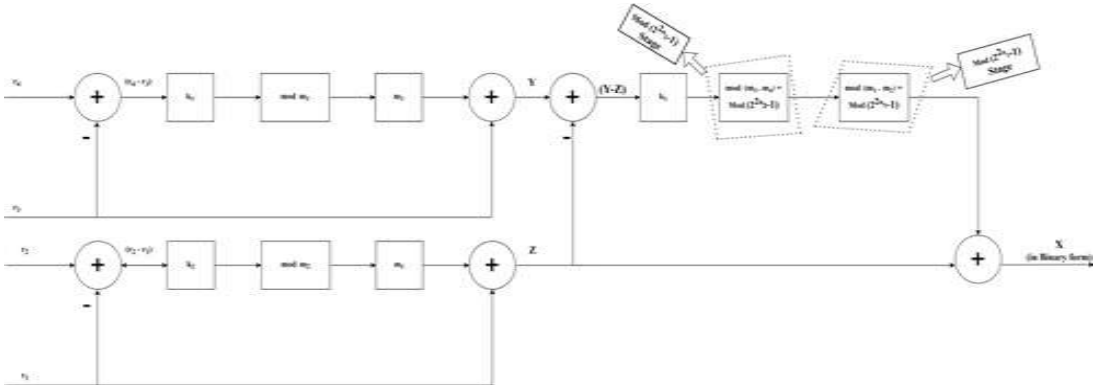


Fig. 2. Proposed block diagram for Forward converter

The proposed approach improves reverse conversion using New CRT-I and New CRT-II with conjugate moduli, based on the works of Skavantzos and Abdallah and Wang. A Mod $2^{n_1}-1$and a Mod $2^{n_1}+1$adder are merged into a single Mod $2^{2n_1}-1$stage, and similarly a Mod $2^{n_2}-1$and a Mod $2^{n_2}+1$adder into a Mod $2^{2n_2}-1$stage, enhancing area and delay performance. Figures 3(a) and 3(b) present the proposed New CRT-I and New CRT-II architectures. Unlike MRC, which is sequential, CRT, New CRT-I, and New CRT-II operate in parallel, making the proposed methods suitable for high-speed reverse conversion.



(a)



(b)

Fig. 3. Proposed block diagram for Reverse converter

(a) With New CRT-I (b) With New CRT-II

In the final stage, the proposed approach presents a detailed block diagram of the Residue Number System (RNS), offering a comprehensive view of the system architecture. Beyond illustrating efficient forward and reverse conversion, the design integrates these stages to form a balanced and adaptive RNS framework that enhances overall performance across diverse applications.

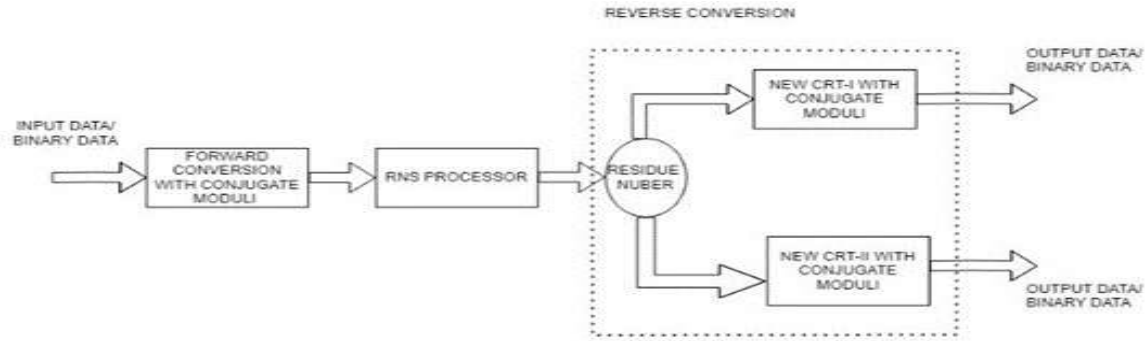


Fig. 4. Proposed block diagram for RNS System

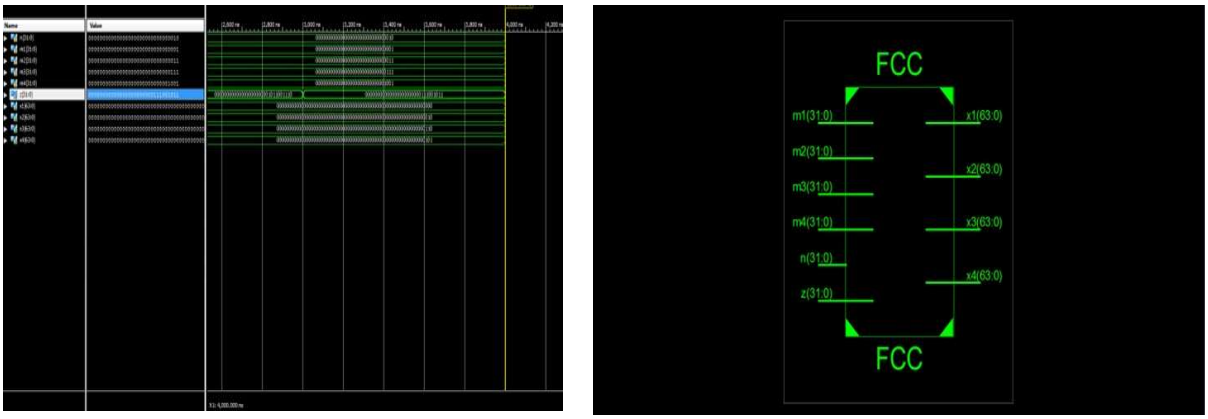
The block diagram comprises forward conversion using conjugate moduli, an RNS processor, and advanced reverse conversion based on New CRTs with conjugate moduli. In this work, only the forward and reverse conversion stages are implemented. The integrated architecture highlights the versatility of the proposed RNS framework for digital signal processing and cryptographic applications, as shown in Fig. 4.

IV. RESULTS & DISCUSSION

The results were verified using Xilinx ISE 14.7 with a Virtex-7 FPGA (xc7vx330t-3ffg1157). Forward and reverse conversion techniques for the Residue Number Systemincluding CRT, MRC, New CRT-I, New CRT-II, and the proposed conjugate moduli setwere implemented in Verilog HDL, compiled, and simulated using the ISIM simulator. The designs were then synthesized to obtain design summaries, including area (slices) and delay (ns) for comparison. Technical schematics illustrating the required blocks and internal connections were also generated for each conversion technique. Using the targeted device, the following results were obtained.

1.2 Forward Conversion

The analog/digital input converted into residue number by using the technic called Forward Conversion and its logic written in Verilog HDL code. It is compiled, simulated and synthesized. For each moduli set mentioned in the Table.1, Verilog HDL code written, simulated and synthesized successfully. For verifying simulation results, the given moduli set is $\{m_1, m_2, m_3, m_4\}$ $=\{2^n - 1, 2^n, 2^n + 1, 2^{2n} + 1\}=\{2^2 - 1, 2^2, 2^2 + 1, 2^{2.2} + 1\} = \{3,4,5,17\}$ for n=2 and the given decimal input is $X = 718$ after executing it, obtained result i.e. resultant residue set $X = \{x_1, x_2, x_3, x_4\} = \{1,2,3,4\}$ corresponding simulation results verified. After simulation, it was synthesized and technical schematic also obtained.



(a) Simulation results (b) Technical schematic

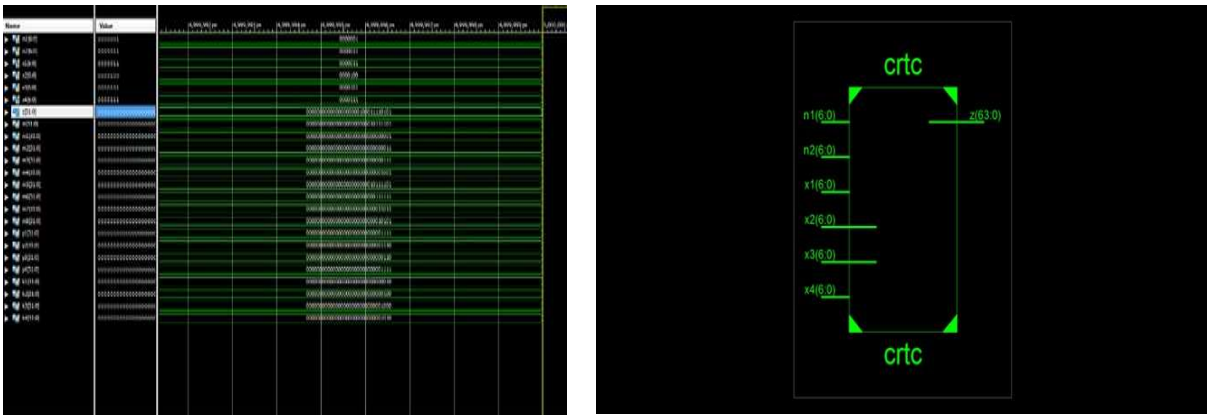
Fig. 5. Proposed forward converter with Conjugate moduli set(FCC)

For verifying simulation results, the proposed conjugate moduli set and scaled down moduli set, given is $\{m_1, m_2, m_3, m_4\}$ $=\{2^{n_1} - 1, 2^{n_1} + 1, 2^{n_2} - 1, 2^{n_2} + 1\}=$ $\{2^3 - 1, 2^3 + 1, 2^7 - 1, 2^7 + 1\} = \{7,9,31,33\} = \{7,3,31,11\}$ for $n_1 = 3$ &$n_2 = 7$ and the given decimal input is $X = 4250$ after this obtained result i.e. resultant residue set $X = \{x_1, x_2, x_3, x_4\} = \{1,2,3,4\}$ corresponding simulation result shown in Fig.5.(a). After simulation, it was synthesized and technical schematic also obtained and it is shown in Fig.5. (b).

4.2 Reverse conversion

The residue number converted back to analog/digital output by using the technic called Reverse Conversion by using the methods called CRT, MRC, New CRT-I and New CRT-II.

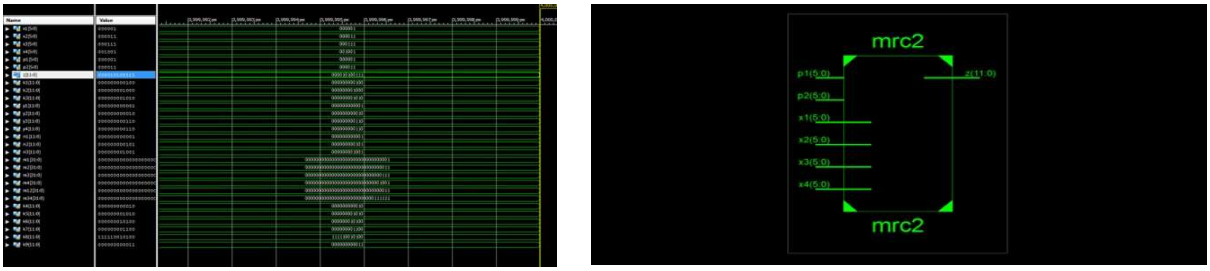
Chinese Remainder Theorem (CRT). The residue number after processing residue arithmetic unit converted back to analog/digital output by using the technic called Reverse Conversion and its logic written in Verilog HDL code. It is compiled, simulated and synthesized. For each moduli set mentioned in the Table.1, Verilog HDL code written, simulated and synthesized successfully. For verifying simulation results, the given moduli set is $\{m_1, m_2, m_3, m_4\}$ $=\{2^n - 1, 2^n, 2^n + 1, 2^{n+1} - 1\}=\{2^2 \quad 1, 2^2, 2^2 \; ; \; 1, 2^{2+1} \quad 1\} = \{3,4,5,7\}$ for n=2 and the given residue set $X = \{x_1, x_2, x_3, x_4\} = \{1,2,3,4\}$ after executing it, obtained result i.e. resultant decimal output is $X = 298$ corresponding simulation results verified. After simulation, it was synthesized and technical schematic also obtained.For each different moduli sets shown in Table.1.and different residue set inputs are given, and corresponding decimal output obtained like above CRT results obtained for each different case.



(a) Simulation results (b) Technical schematic

Fig. 6. Proposed Chinese Remainder Theorem with Conjugate moduli set (CRTC)

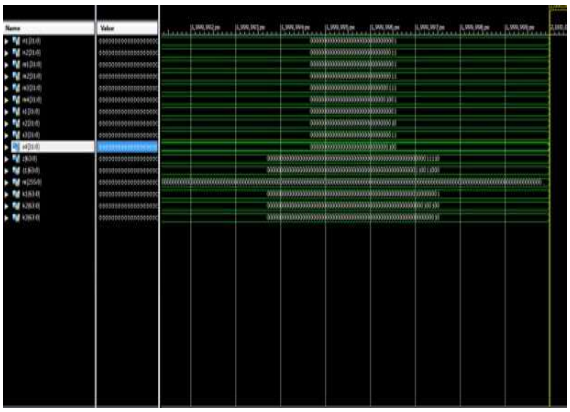
These values are shown in performance comparison.For verifying simulation results, the proposed conjugate moduli set and scaled down moduli set, given is $\{m_1, m_2, m_3, m_4\}$ $=\{2^{n_1}-1, 2^{n_1}+1, 2^{n_2}-1, 2^{n_2}+1\}=$ $\{2^3-1, 2^3+1, 2^7-1, 2^7+1\} = \{7,9,31,33\} = \{7,3,31,11\}$ for $n_1 = 3$ &$n_2 = 7$ and the given decimal input is $X = 4250$ after this obtained result i.e. resultant residue set $X = \{x_1, x_2, x_3, x_4\} = \{1,2,3,4\}$ corresponding simulation result shown and After simulation, it was synthesized by the above mentioned selected targeted device and obtained the Synthesis and technical schematic also obtained and it is shown in Fig.6.**Mixed Radix Conversion (MRC).**For verifying simulation results, the proposed conjugate moduli set and scaled down moduli set, given is $\{m_1, m_2, m_3, m_4\}$ $=\{2^{n_1}-1, 2^{n_1}+1, 2^{n_2}-1, 2^{n_2}+1\}=$ $\{2^3-1, 2^3+1, 2^7-1, 2^7+1\} = \{7,9,31,33\} = \{7,3,31,11\}$ for $n_1 = 3$ &$n_2 = 7$ and the given decimal input is $X = 4250$ after this obtained result i.e. resultant residue set $X = \{x_1, x_2, x_3, x_4\} = \{1,2,3,4\}$ corresponding simulation result shown in Fig.7.(a). After simulation, it was synthesized by the above mentioned selected targeted device and obtained the Synthesis report and technical schematic also obtained and it is shown in Fig.7. (b).



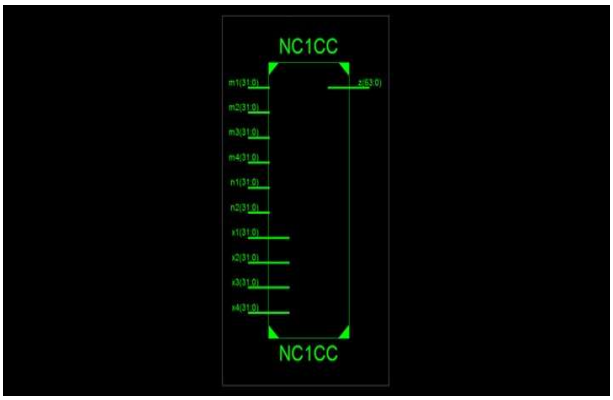
(a) Simulation results (b) Technical schematic

Fig. 7.Proposed Mixed Radix Conversion with Conjugate moduli set (MRCC)

New Chinese Remainder Theorem-I (New CRT-I). For verifying simulation results, the proposed conjugate moduli set and scaled down moduli set, given is $\{m_1, m_2, m_3, m_4\}$ $=\{2^{n_1}-1, 2^{n_1}+1, 2^{n_2}-1, 2^{n_2}+1\}=$ $\{2^3-1, 2^3+1, 2^7-1, 2^7+1\} = \{7,9,31,33\} = \{7,3,31,11\}$ for $n_1 = 3$ &$n_2 = 7$ and the given decimal input is $X = 4250$ after this obtained result i.e. resultant residue set $X = \{x_1, x_2, x_3, x_4\} = \{1,2,3,4\}$ corresponding simulation result shown in Fig.8.(a). After simulation, it was synthesized by the above mentioned selected targeted device and obtained the Synthesis report and technical schematic also obtained and it is shown in Fig.8. (b).



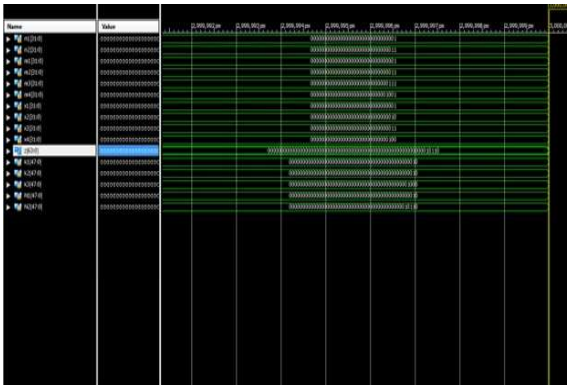
(a) Simulation results



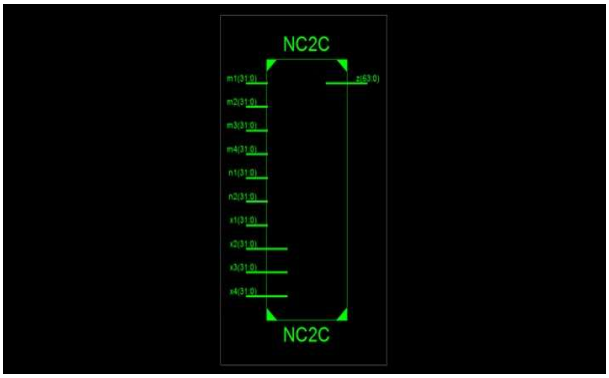
(b) Technical schematic

Fig. 8. Proposed New CRT-I with Conjugate moduli set (NCIC)

New Chinese Remainder Theorem-II (New CRT-II).down moduli set, given is $\{m_1, m_2, m_3, m_4\}$ $=\{2^{n_1}-1, 2^{n_1}+1, 2^{n_2}-1, 2^{n_2}+1\}=$ $\{2^3-1, 2^3+1, 2^7-1, 2^7+1\} = \{7,9,31,33\} = \{7,3,31,11\}$ for $n_1 = 3$ &$n_2 = 7$ and the given decimal input is $X = 4250$ after this obtained result i.e. resultant residue set $X = \{x_1, x_2, x_3, x_4\} = \{1,2,3,4\}$ corresponding simulation result shown in Fig.9.(a). After simulation, it was synthesized by the above mentioned selected targeted device and obtained the Synthesis and technical schematic also obtained and it is shown in Fig.9. (b).



(a) Simulation results



(b) Technical schematic

Fig. 9. Proposed New CRT-II with Conjugate moduli set (NCIIC)

From the literature survey different moduli sets are considered for discussion, these are also shown in Table.1, and decimal input given in forward conversion and also the proposed conjugate moduli sets and decimal input are given obtained the results. On the other hand, reverse conversion methods result such as CRT, CRTC, MRC, MRCC, NCI, NCIC, NCII and NCIIC also obtained and explained.

V. PERFORMANCE COMPARISON

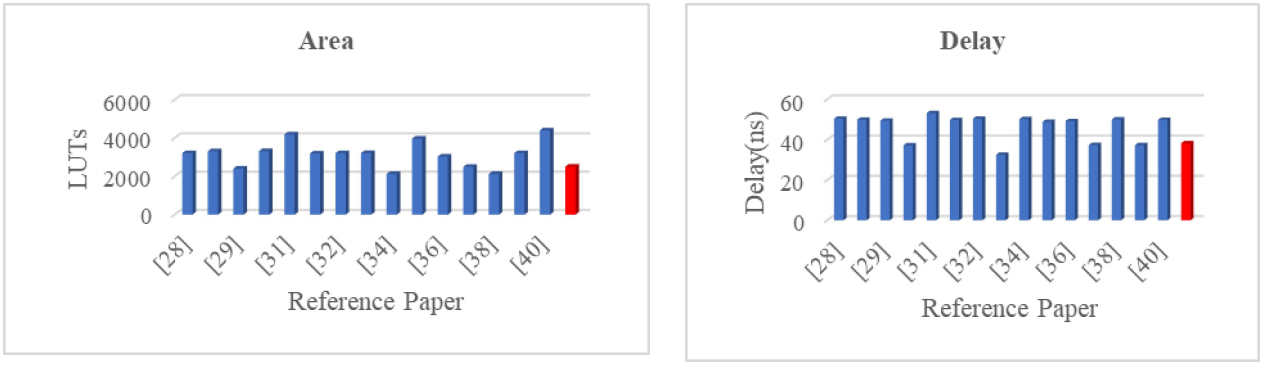
This section evaluates the performance comparison of the proposed conjugate moduli set in forward conversion and reverse conversion. Table.2 outlines the hardware complexity and delay of forward conversion and results depicted shown in Fig.10. Performance improvement can be calculated with the following relationship in Eq.4.

$$Improvement = \frac{Value_{Competitive} - Value_{Proposed}}{Value_{Proposed}} X\ 100\% \quad (4)$$

Table 2. Comparison of Forward conversion for different Moduli sets

The Table 2 shows the conversion time and hardware cost of the proposed conjugate moduli set-based converters in comparison to those found in the literature. In summary, Table 2 shows that the proposed converters not only improve delay performance but also require less hardware than the converters presented in Table 1. The results were verified using Xilinx ISE 14.7 on a Virtex-7 FPGA (xc7vx330t-3ffg1157). The forward and reverse RNS conversion techniques i.e. CRT, MRC, New CRT-I, New CRT-II, and the proposed conjugate moduli setwere implemented in Verilog HDL and simulated using ISIM. The proposed forward converter achieves approximately 26.32% area savings and 19.19% delay reduction, as shown in Fig. 11, with area measured in slices and delay in nanoseconds (Table 1). The reverse conversion performance, evaluated in Tables 3–6 and Figs. 11–14, indicates that the proposed method attains 62.03% area improvement and 30.74% delay reduction for CRT. The overall comparison shows that CRT provides superior reverse conversion performance compared to MRC, New CRT-I, and New CRT-II, as illustrated in Fig. 11. The Table 3. Performance Comparison of CRT for different Moduli sets

Year	**Area (LUTs)**	**Delay (ns)**	**Area Performance Improvement**	**Delay Performance improvement**
[28]	3211	50.424	**28.337**	**31.728**
[29]	3311	49.933	**32.334**	**30.445**
[29]	2405	49.476	-3.877	**29.251**
[30]	3315	37.218	**32.494**	-2.772
[31]	4188	53.209	**67.386**	**39.003**
[32]	3192	49.791	**27.578**	**30.074**
[32]	3211	50.424	**28.337**	**31.728**
[33]	3215	32.528	**28.497**	-15.024
[34]	2126	50.217	-15.028	**31.187**
[35]	3971	48.882	**58.713**	**27.699**
[36]	3028	49.236	**21.023**	-1.450
[37]	2496	37.368	-0.240	-2.380
[38]	2126	50.044	-15.028	**30.735**
[39]	3211	37.279	**28.337**	-2.612
[40]	4402	49.881	**75.939**	**30.09**
Proposed	2502	38.279		



(a) Area (b) Delay

Fig. 10. Performance comparison for Forward conversion

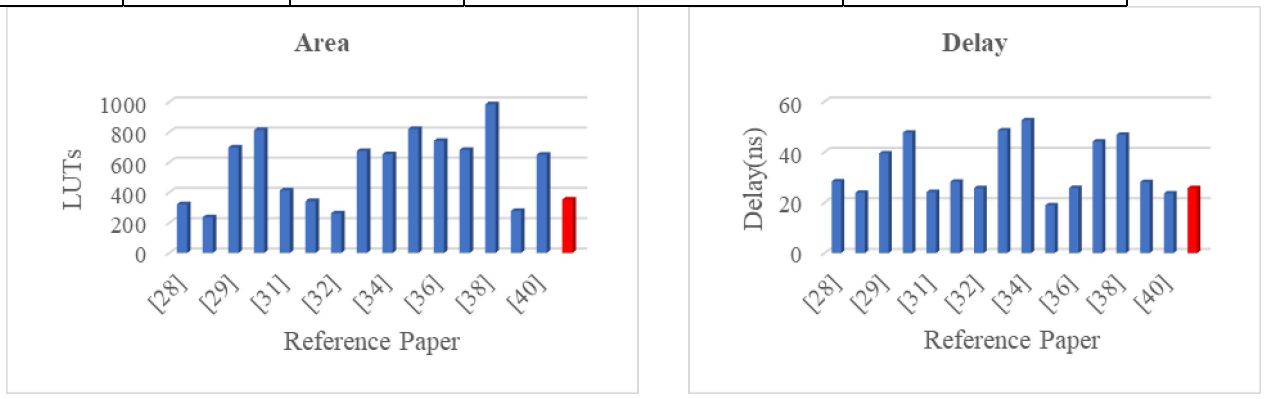
The Fig. 11 further confirms that the proposed method improves both area and delay for the CRT-based reverse conversion. The performance comparison for MRC, summarized in Table 4, evaluates area in terms of look-up tables (LUTs) and delay in nanoseconds. Positive values indicate area improvement, while negative values denote inferior performance compared to existing moduli sets. As shown in Table 4, the proposed method achieves an area improvement of approximately 13.41% but exhibits a delay degradation of about 24.02% relative to the available moduli sets. The Table 4 presents the area (LUTs) and delay (ns) results for the MRC technique. As MRC is a sequential approach, the proposed method shows some improvement in hardware area but exhibits degraded delay performance, indicated by negative values. This confirms that MRC is unsuitable for high-speed applications due to its sequential nature. The area and delay results from Table 4 are illustrated in Figs. 12(a) and 12(b), where blue bars represent reference methods and red bars indicate the proposed approach for comparison.

Table 4 summarizes the area and delay results for the MRC technique. Since MRC is a sequential approach, the proposed method offers some hardware area improvement but shows degraded delay performance, indicated by negative values. This confirms that MRC is not suitable for high-speed applications. The area and delay results are illustrated in Figs. 12, where blue bars represent reference methods and red bars indicate the proposed approach for comparison.

The performance comparison shown in Fig. 12 indicates that, for the MRC technique, the proposed method achieves improvement in area but exhibits inferior delay performance when compared to existing moduli sets. The evaluation of New CRT-I, summarized in Table 5, considers area in terms of LUTs and delay in nanoseconds. The results demonstrate that the proposed approach provides approximately 23.52% improvement in area and 22.73% improvement in delay, with the corresponding comparison illustrated in Fig. 18. The findings further indicate that New CRT-I, as an advanced technique, benefits from the proposed method in both area and delay, as depicted in Figs. 13(a) and 13(b), where blue bars represent reference methods and red bars denote the proposed approach.

(c) Table 3. Performance Comparison of CRT for differentModuli sets

Year	Area(LUTs)	Delay(ns)	AreaPerformanceimprovement	DelayPerformanceimprovement
[28]	324	28.368	-8.215	**10.446**
[29]	237	23.847	-32.861	-7.156
[29]	698	39.478	**97.734**	**53.701**
[30]	814	47.701	**130.595**	**85.715**
[31]	413	24.138	**16.997**	-6.023
[32]	343	28.239	-2.833	**9.944**
[32]	263	25.681	-25.496	-0.016
[33]	675	48.612	**91.218**	**89.262**
[34]	654	52.625	**85.269**	**104.886**
[35]	821	19.021	**132.578**	-25.945
[36]	742	25.746	**110.198**	-9.706
[37]	682	44.184	**93.201**	**72.023**
[38]	985	46.863	**179.037**	**82.453**
[39]	279	28.134	-20.963	**9.535**
[40]	650	23.62	**84.136**	-8.04
Proposed	353	25.685		

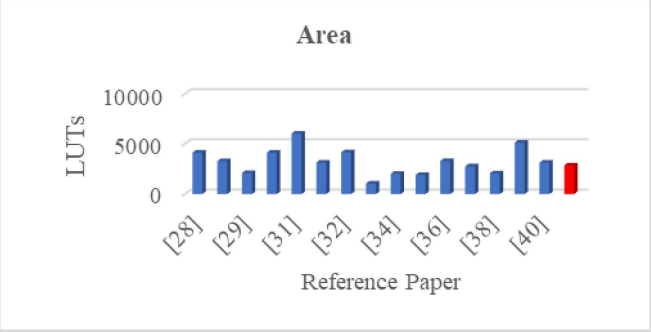


(a) Area (b) Delay

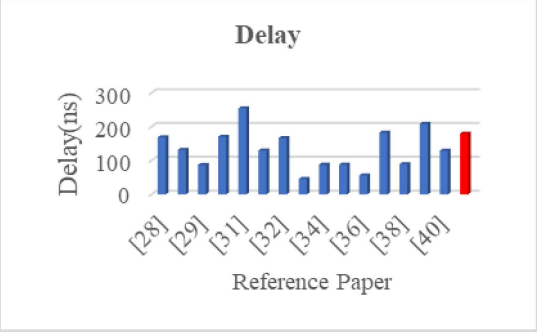
Fig. 11. Performance comparison for CRT

Table 4. Performance Comparison of MRC for differentModuli sets

Year	Area(LUTs)	Delay(ns)	AreaPerformanceimprovement	DelayPerformanceimprovement
[28]	4714	123.215	**38.606**	**37.652**
[29]	3378	121.609	-0.676	**35.858**
[29]	4771	83.5477	**40.282**	-6.663
[30]	3305	125.695	-2.823	**40.423**
[31]	4840	118.736	**42.311**	**32.648**



(a) Area

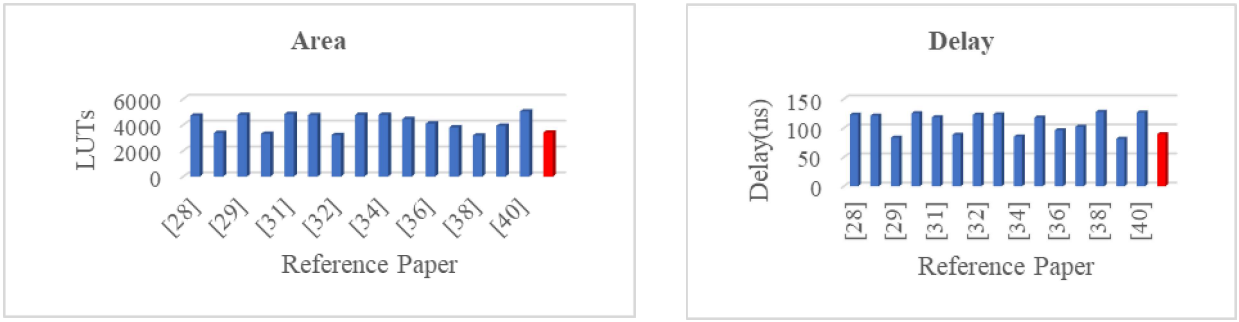


(b) Delay

[32]	4754	88.512	**39.782**	-1.117
[32]	3208	123.215	-5.675	**37.652**
[33]	4771	123.644	**40.282**	**38.131**
[34]	4773	85.496	**40.341**	-4.487
[35]	4451	118.147	**30.873**	**31.99**
[36]	4103	96.418	**20.641**	**8.832**
[37]	3802	102.352	**11.791**	**14.344**
[38]	3178	127.921	-6.557	**42.909**
[39]	3926	81.526	**15.437**	-8.922
[40]	5042	126.894	**48.251**	**41.762**
Proposed	3401	89.512		

Fig. 12. Performance comparison for MRC

Table 5. Performance Comparison of New CRT-I for differentModuli sets

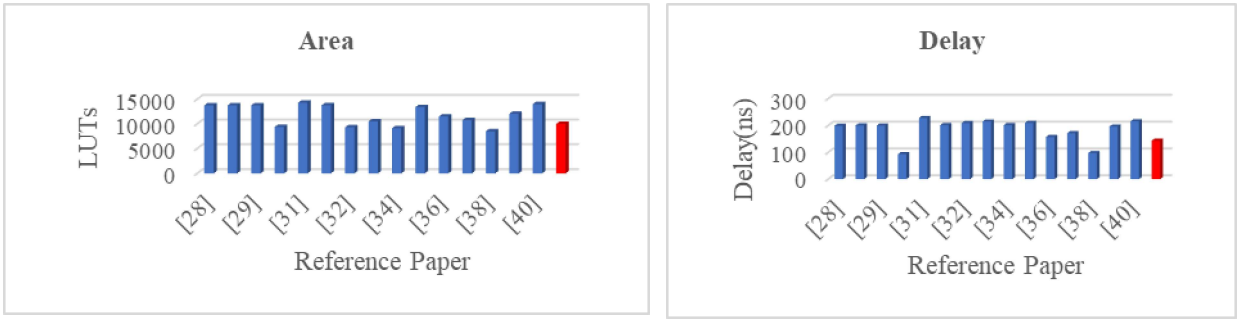


(a) Area (b) Delay

Fig. 13. Performance comparison for New CRT-I

The comparison in Fig. 13 shows that the proposed method improves area but degrades delay for the MRC technique. The performance evaluation of New CRT-II in Table 6 indicates an area improvement of approximately 18.71% and a delay improvement of 27.23%, as illustrated in Fig. 14. The advanced New CRT-II technique thus achieves better performance with reduced hardware requirements, with area and delay results depicted in Figs. 14(a) and 14(b).The results in Fig. 14 show that the proposed New CRT-II method achieves improvements in both area and delay compared to existing moduli sets. The overall analysis indicates that the proposed conjugate moduli set enhances hardware efficiency and reduces delay in both forward and reverse conversion, except for the MRC technique.

Table 6. Performance Comparison of New CRT-II for differentModuli sets



(a) Area (b) Delay

Fig. 14. Performance comparison for New CRT-II

VI. CONCLUSION & FUTURE SCOPE

In conclusion, the proposed conjugate moduli set $\{2^{n_1}-1, 2^{n_1}+1, 2^{n_2}-1, 2^{n_2}+1, 2^{n_3}-1, 2^{n_3}+1, \ldots\ldots\ldots 2^{n_L}-1, 2^{n_L}+1\}$ for forward and reverse conversion procedures in Residue Number Systems shows significant performance gains. The results obtained using Xilinx ISE 14.7 on a Virtex-7 FPGA show improved efficiency for CRT, MRC, New CRT-I, and New CRT-II. The forward conversion achieves a 2.32% area improvement and a 5.36% delay reduction, while the reverse conversion achieves a 5.23% area improvement and a 5.64% latency reduction. The proposed conjugate moduli set demonstrates clear benefits for signal and radar signal processing applications.

The future work includes extending the proposed moduli set to cryptography and error correction, integrating it with advanced FPGA technologies, and validating performance through real-world implementations.

REFERENCES

[1]S. C. Yang, “Toward a wireless world,” IEEE Technol. Soc. Mag., vol. 26, no. 2, pp. 32–42, Jun. 2007.
[2]R. Schneiderman, “DSPs evolving in consumer electronics applications,” IEEE Signal Process. Mag., vol. 27, no. 3, pp. 6–10, May 2010.
[3]T. Stouraitis and V. Paliouras, “Considering the alternatives in lowpower design,” IEEE Circuits Devices Mag., vol. 17, no. 4, pp. 23–29,Jul. 2001.
[4]H. L. Garner, “The residue number system,” IRE Trans. Electron. Comput., vol. 8, no. 2, pp. 140–147, 1959.
[5] C.-H. Chang, A. S. Molahosseini, A. A. E. Zarandi, and T. F. Tay, “Residue number systems: A new paradigm to datapath optimization for low-power and high-performance digital signal processing applications,” IEEE Circuits Syst. Mag., vol. 15, no. 4, pp. 26–44, 4th Quart. 2015.
[6]Bajard, Jean-Claude, Nicolas Meloni, and Thomas Plantard. "Efficient RNS bases for cryptography." *Proceedings of IMACS 2005 World Congress, Paris, France (July 2005)*. 2005.
[7]S. Yen, S. Kim, S. Lim and S. Moon, “RSA Speedup with Chinese Remainder Theorem Immune against Hardware Fault Cryptanalysis,” IEEE Transactions on Computers, vol. 52, no. 4, pp. 461-472, 2003.
[8]J. Ramirez, et al., “Fast RNS FPL-Based Communications Receiver Design and Implementation," Proceedings of the 12th Int’l Conf. Field Programmable Logic, pp. 472-481, 2002.
[9]R. Conway and J. Nelson, “Improved RNS FIR Filter Architectures,” IEEE Transactions On Circuits and Systems II, Vol. 51, No. 1, pp. 26-28, 2004
[10]W. Wei et al., “RNS application for digital image processing,” Proceedings of the 4th IEEE international workshop on system-on-chip for real time applications, Canada, pp. 77-80, 2004.
[11]Clarke, John. *The Chinese remainder theorem and multi-PRF radars*. Royal Signals & Radar Establishment, 1984.
[12]Oke, Afeez Adeshina, et al. "RESIDUE NUMBER SYSTEM BASED APPLICATIONS: A LITERATURE REVIEW." *Annals. Computer Science Series* 19.1 (2021).
[13]Mohan, PV Ananda, and PV Ananda Mohan. *Residue Number Systems*. Cham, Switzerland: Birkhäuser, 2016.
[14]A. Omondi and B. Premkumar, “Residue Number System: Theory and Implementation,” Imperial College Press 2007, ISBN 978-1-86094-866-4.
[15]G Navi, K., Molahosseini, A.S. and Esmaeildoust, M., 2010. How to teach residue number system to computer scientists and engineers. IEEE Transactions on Education, 54(1), pp.156-163.
[16]Taylor, "Residue Arithmetic A Tutorial with Examples," in Computer, vol. 17, no. 5, pp. 50-62, May 1984, doi: 10.1109/MC.1984.1659138.
[17]Ghassem Jaberipur and Seyed Hamed Fatemi Langroudi,” (4 + 2 logn)ΔG Parallel Prefix Modulo Adder 2^n-3 via Double Representation of Residues in [0,2], IEEE Transactions on Circuits and Systems II: Express Briefs,2015.
[18]Wang, Y., 2000. Residue-to-binary converters based on new Chinese remainder theorems. IEEE Transactions on Circuits and Systems II: Analog and Digital Signal Processing, 47(3), pp.197-205.

[19]A. Nazarov, M. Babenko and E. Golimblevskaia, "Efficient Hardware Implementation of Forward Conversion WNS-RNS on FPGA," *2020 International Conference Engineering and Telecommunication (En&T)*, Dolgoprudny, Russia, 2020, pp. 1-4, doi: 10.1109/EnT50437.2020.9431304.

[20]Nazarov, Anton, Mikhail Babenko, and Elena Golimblevskaia. "Hardware implementation of the reverse conversion RNS-WNS on FPGA." *2020 International Conference Engineering and Telecommunication (En&T)*. IEEE, 2020.

[21]Abdelfattah, Omar. "Data Conversion in Residue Number System." (2011).

[22]Mohan, PV Ananda, and PV Ananda Mohan. *Residue Number Systems*. Cham, Switzerland: Birkhäuser, 2016.

[23]García, Fernando Darío Almeida, et al. "Doppler Estimation for High-Velocity Targets Using Subpulse Processing and the Classic Chinese Remainder Theorem." *arXiv preprint arXiv:2101.11311* (2021).

[24]Chang, Chip-Hong, et al. "Residue number systems: A new paradigm to datapath optimization for low-power and high-performance digital signal processing applications." *IEEE circuits and systems magazine* 15.4 (2015): 26-44.

[25]Chang, Chip-Hong, et al. "Residue number systems: A new paradigm to datapath optimization for low-power and high-performance digital signal processing applications." *IEEE circuits and systems magazine* 15.4 (2015): 26-44.

[26]Skavantzos, A. and Abdallah, M., 1999. Implementation issues of the two-level residue number system with pairs of conjugate moduli. IEEE Transactions on Signal Processing, 47(3), pp.826-838.

[27]G. C. Cardarilli, A. Nanareelli, and M. Re, "Reducing power dissipation in FIR filters using the residue number system," Proceedings of the 43rd IEEE Midwest Symposium on Circuits and Systems, Vol. 2, pp. 320-323, 2000.

[28]Cao, Bin, Chip-Hong Chang, and Thambipillai Srikanthan. "An efficient reverse converter for the 4-moduli set {2/sup n/-1, 2/sup n/, 2/sup n/+ 1, 2/sup 2n/+ 1} based on the new Chinese remainder theorem." IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications 50.10 (2003): 1296-1303.

[29]Mohan, PV Ananda, and A. B. Premkumar. "RNS-to-Binary Converters for Two Four-Moduli Sets $\{2^{n}-1, 2^{n}, 2^{n}+ 1, 2^{{n}+ 1}-1\} $ and $\{2^{n}-1, 2^{n}, 2^{n}+ 1, 2^{{n}+ 1}+ 1\} $." IEEE Transactions on Circuits and Systems I: Regular Papers 54.6 (2007): 1245-1254.

[30]Ananda Mohan, P. V. "New reverse converters for the moduli set." AEU International Journal of Electronics and Communications 62.9 (2008): 643.

[31]Zhang, Wei, and Pepe Siy. "An efficient design of residue to binary converter for four moduli set (2n-1, 2n+ 1, 22n-2, 22n+ 1-3) based on new CRT II." Information Sciences 178.1 (2008): 264-279.

[32]Molahosseini, Amir Sabbagh, et al. "Efficient Reverse Converter Designs for the New 4-Moduli Sets $\{2^{n}-1, 2^{n}, 2^{n}+ 1, 2^{2n+ 1}-1\} $ and $\{2^{n}-1, 2^{n}+ 1, 2^{2n}, 2^{2n}+ 1\} $ Based on New CRTs." IEEE Transactions on Circuits and Systems I: Regular Papers 57.4 (2009): 823-835.

[33]Sousa, Leonel, Samuel Antão, and Ricardo Chaves. "On the Design of RNS Reverse Converters for the Four-Moduli Set ${\bf\{2^{\mmb n}+ 1, 2^{\mmb n}-1, 2^{\mmb n}, 2^{{\mmb n}+ 1}+ 1\}} $." IEEE transactions on very large scale integration (VLSI) systems 21.10 (2012): 1945-1949.

[34]Esmaeildoust, Mohammad, et al. "Efficient RNS to binary converters for the new 4-moduli set {2n, 2n+ 1-1, 2n-1, 2n-1-1}." IEICE Electronics Express 9.1 (2012): 1-7.

[35]Bader, Mansour, Andraws Swidan, and Mazin Al-hadidi. "NEW NON-COPRIME CONJUGATE-PAIR BINARY TO RNS MULTI-MODULI FOR RESIDUE NUMBER SYSTEM." Computer Science & Information Technology (2017): 105.

[36]Ananda Mohan, P. V. "Reverse Converters for the Moduli Set 2^ n, 2^ n-1-1, 2^ n-1, 2^ n+ 1-1\}(n\, Even) 2 n, 2 n-1-1, 2 n-1, 2 n+ 1-1 (n Even)." Circuits, Systems, and Signal Processing 37 (2018): 3605-3634.

[37]Jaiswal, Ritesh Kumar, Raj Kumar, and Ram Awadh Mishra. "Area Efficient Memoryless Reverse Converter for New Four Moduli Set {2 n− 1, 2 n− 1, 2 n+ 1, 2 2 n+ 1− 1}." Journal of Circuits, Systems and Computers 27.05 (2018): 1850075.

[38]Obeidi Daghlavi, Mohammad, Mohammad Reza Noorimehr, and Mohammad Esmaeildoust. "Efficient two-level reverse converters for the four-moduli set {2 n− 1, 2 n–1, 2 n− 1–1, 2 n+ 1–1}." Analog Integrated Circuits and Signal Processing 108 (2021): 75-87.

[39]Akbari, Ali, et al. "A New High-Speed, Low-Area Residue-to-Binary Converter For the Moduli Set {2 4 n, 2 2 n+ 1, 2 n+ 1, 2 n-1} Based on CRT-1." Circuits, Systems, and Signal Processing 40.11 (2021): 5773-5786.

[40]Obeidi Daghlavi, M., Noorimehr, M.R. & Esmaeildoust, M. Efficient two-level reverse converters for the four-moduli set {2n−1, 2n–1, 2n−1–1, 2n+1–1}. Analog Integr Circ Sig Process 108, 75–87 (2021).