# AN OPTIMISED IMPLEMENTATION OF ADAPTIVE RNS USING POWER-AWARE CRT

Reference NO. IJME 1380, DOI: 10.5750/ijme.v1i1.1380

**Bentipalli Sekhar*,** Research Scholar, JNTU-Gurajada-Vizianagaram College of Engineering, India, **G Appala Naidu,** Assistant Professor in ECE, JNTU-Gurajada-Vizianagaram College of Engineering, India and **K. Babulu,** Professor in ECE, JNTU-Gurajada-Vizianagaram College of Engineering, India

*Corresponding author. Bentipalli Sekhar (Email): sekharmana@gmail.com

KEY DATES: Submission date: 25.12.2023 / Final acceptance date: 27.02.2024 / Published date: 12.07.2024

## SUMMARY

In order to get an efficient comprehensive analysis on Doppler estimation in RADAR; need an enhanced arithmetic formulation procedure for density, power and latency optimisations. Modular adders and multipliers are very crucial components in the performance of residue number system-based applications. The Residue Number System (RNS) is a non-positional number system that allows parallel computations without transfers between digits. However, some operations in RNS require knowledge of the positional characteristic of a number. Among these operations is the conversion from RNS to the positional number system. The methods of reverse conversion for general form moduli based on the Chinese remainder theorem and the mixed-radix conversion are considered, as well as the optimized methods for special form moduli. A modified New CRT-I & New CRT-II with conjugate moduli set is considered to implement adder, multipliers and subtractions with optimised algorithms. This paper mainly deals with the conversion of numbers from binary to RNS as well RNS to binary with the specific modulo {2^n±k} which proves this new method. Modified Radix16 booth encoding algorithm and square carry bypass adder are used in implementation of RNS system to reduce parameter constraints.

## KEYWORDS

Residue Number System, Chinese Remainder Theorems, Doppler, CONJUGATE PAIRS, Radix16 Booth Encoding, Square Carry Bypass Adder

## NOMENCLATURE

| | |
|---|---|
| RNS | Residue Number System |
| CRT | CHINESE REMAINDER Theorem |
| DSP | Digital Signal Processing |
| F | Frequency |
| CSAs | Carry Save Adder |

## 1. INTRODUCTION

Automatic numbering systems must not be used. The residue number system (RNS) serves as a non-weighted representation, rooted in the expression of any number using relatively prime positive integers known as moduli. The collective product of all moduli delineates the dynamic range wherein numbers within this spectrum are uniquely represented. Each modulus operates independently from others during addition, subtraction, and multiplication, leading to enhanced computational efficiency. The computational pathway for each modulus, termed a channel, facilitates operations with relative independence. For an RNS representation employing L moduli, L parallel channels are established. This parallelism significantly reduces the time required for computationally intensive arithmetic applications relying on these operations. Increasing the number of moduli enhances parallelism, thereby shortening word-lengths for each channel and expediting processing speed. While three-moduli sets suffice for certain digital signal processing (DSP) applications, others necessitate higher levels of parallelism unattainable with such sets. In response, several new residue-to-binary converters have been introduced, known as the New CRT's I and II. These converters, based on novel fast conversion theorems distinct from traditional methods, represent a notable advancement since the seminal work of Szabo and Tanaka. Compared to traditional CRT and Modified Residue Number System (MRC) approaches, the New CRT's require smaller modulo adders and involve smaller numbers, resulting in increased computational speed. Given these advantages, it is anticipated that the New CRT's will supplant both CRT and MRC methods across various applications.

 

Considering the widespread use of CRT, it is expected that many applications in digital signal processing, communication, and computer arithmetic will benefit from the introduction of the New CRT's. Moreover, current techniques for complex RNS operations, such as divisions and scaling, which rely on CRT or MRC approaches, are poised to benefit significantly from the algorithms presented here. Hence, the conventional understanding of RNS-based arithmetic is poised for a transformative challenge. The Residue Number System (RNS) is a numerical representation scheme distinct from traditional positional systems like decimal or binary. In RNS, numbers are represented by their residues modulo a set of pairwise coprime moduli, known as the moduli set. Each residue corresponds to the remainder obtained when dividing the number by its respective modulus. This approach enables parallel computation as arithmetic operations can be performed independently on each residue without carry propagation. RNS is particularly advantageous in applications requiring high-speed arithmetic operations such as digital signal processing, cryptography, and error control coding. Key aspects of RNS include the careful selection of moduli to ensure unique representations, the utilization of modular arithmetic for computation, and specialized techniques for overflow and error handling. Its parallelism and efficiency make RNS a valuable tool in modern computing systems, offering an alternative approach to numerical representation and computation. The Residue Number System (RNS) plays a pivotal role in the Chinese Remainder Theorem (CRT), a fundamental mathematical concept with diverse applications ranging from cryptography to error detection and correction. In the context of CRT, RNS enables efficient and parallel computation by breaking down complex arithmetic operations into simpler modular computations. The CRT states that if we have a system of congruences with pairwise coprime moduli, then any set of residues modulo these moduli uniquely determines a residue modulo their product. This property allows us to decompose computations modulo each individual modulus, perform them independently, and then combine the results using the CRT to obtain the final solution. This approach not only offers significant computational advantages, such as reducing the computational complexity of large integer arithmetic, but also provides robustness against errors and faults, as it allows for error detection and correction at the residue level. Thus, the combination of RNS and CRT forms a powerful framework for efficient and reliable arithmetic operations in various practical applications.

Residue Number System (RNS) provides a practical implementation of the CRT in computer arithmetic. In RNS, numbers are represented by their residues modulo a set of pairwise coprime moduli. The use of RNS enables efficient and parallel computation by breaking down arithmetic operations into simpler modular computations. Specifically, complex arithmetic operations can be decomposed into operations modulo each individual modulus in the RNS, which can then be computed independently. This parallelism is advantageous for high-speed arithmetic operations and can significantly improve computational efficiency, especially in applications requiring intensive arithmetic processing, such as cryptography and digital signal processing. The key benefit of using RNS in conjunction with the CRT lies in its ability to handle large integers and complex arithmetic operations with reduced computational complexity. By exploiting the properties of modular arithmetic and the CRT, computations can be distributed across multiple moduli, leading to faster and more efficient processing. Additionally, the decomposition of computations into residue-level operations provides inherent error detection and correction capabilities, as errors occurring in one modulus can be detected and corrected independently without affecting other residues.

Practical implementations of RNS with CRT often involve careful selection of moduli to ensure efficiency and reliability. Techniques such as optimal modulus selection, dynamic modulus scaling, and error detection and correction algorithms tailored to the characteristics of RNS are commonly employed to maximize performance and robustness. With combination of Residue Number System with the Chinese Remainder Theorem forms a powerful framework for efficient and reliable arithmetic operations in various applications, making it a valuable tool in modern computing systems where speed, efficiency, and accuracy are paramount.

The contribution of our paper lies in providing a comprehensive study on the Residue Number System (RNS) and its applications, addressing key challenges and exploring potential enhancements in the field. Tthorough understanding of RNS, covering fundamental concepts such as moduli selection, data transformations, and decoding algorithms. By providing a detailed overview of RNS operations, we contribute to expanding knowledge and promoting the adoption of this innovative numerical representation scheme. With moduli selection and data transformations as critical bottlenecks in the widespread adoption of RNS. By recognizing these challenges, we contribute to guiding future research efforts towards addressing these issues and improving the efficiency and effectiveness of RNS-based systems. With the diverse applications of RNS across various computer-related domains, including digital signal processing, cryptography, and error control coding. By showcasing the versatility and potential impact of RNS, we contribute to fostering innovation and driving advancements in these fields. Through practical examples and illustrations, we demonstrate the translation of conventional data formats into RNS form and vice versa. By providing tangible demonstrations of RNS applications.With the paper contributes to advancing the state-of-the-art in RNS technology by providing insights, addressing challenges, and outlining future research directions in this field. Through our comprehensive study, we aim to foster

innovation and promote the adoption of RNS as a valuable tool in various computational applications.

## 2. LITERATURE SURVEY

A literature survey serves as a cornerstone in academic research, offering a comprehensive overview of existing studies, methodologies, and findings within a specific field or topic. Conducting a thorough literature survey is essential for researchers to identify gaps in knowledge, understand the current state-of-the-art, and contextualize their own work within the broader academic discourse. By examining a wide range of scholarly sources such as academic journals, conference proceedings, books, and dissertations, researchers can gain insights into the evolution of ideas, methodologies, and debates surrounding their research area. Moreover, a well-executed literature survey not only provides a foundation for conceptualizing research questions but also enables researchers to critically evaluate existing approaches and formulate novel contributions to advance the field.

"Hyperledger Fabric: A Distributed Operating System for Permissioned Blockchains" by Elli Androulaki et al. presents a comprehensive framework for permissioned blockchains, addressing crucial aspects of distributed systems. Dongxu Huang et al.'s work on "TiDB: A Raft-based HTAP Database" introduces an innovative approach to hybrid transactional/analytical processing databases, contributing to the advancement of database technology. "Everyone Loves File: Oracle File Storage Service" by Bradley C. Kuszmaul et al. explores the Oracle File Storage Service, shedding light on advancements in cloud storage solutions. On the topic of consensus mechanisms, X. Xu et al.'s "Weighted RAFT: An Improved Blockchain Consensus Mechanism for Internet of Things Application" proposes enhancements to blockchain consensus mechanisms tailored for IoT applications. Additionally, papers such as "Totally Fault Tolerant RNS based FIR Filters" by Pontarelli et al. and "An Overview of Residue Number System" by Aremu and Gbolagade delve into the application and theoretical aspects of Residue Number System (RNS), offering insights into its use in fault-tolerant systems and numerical computation.

Furthermore, the literature survey includes studies focusing on cryptographic techniques and data security. "CRT and ART Based Watermarking Scheme in DCT Domain" by Priyanka et al. and "Reversible Watermarking using Residue Number System" by Atta-Ur-Rahman et al. explore watermarking techniques utilizing Residue Number System, contributing to the field of digital image and multimedia security. Additionally, Azizifard et al.'s works on "Information Steganography within 3D Images" and "Data Steganography on VoIP through Combination of Residue Number System and DNA Sequences" present novel approaches to information hiding, leveraging RNS in diverse applications. Moreover, Baagyere et al.'s research on "A MultiLayered Data Encryption and Decryption Scheme Based on Genetic Algorithm and Residual Numbers" and "Application of Residue Number System to Smith-Waterman Algorithm" demonstrates the versatility of RNS in encryption and bioinformatics, respectively. Lastly, Babatunde et al.'s "An Algorithm for a Residue Number System Based Video Encryption System" contributes to video encryption techniques, showcasing the applicability of RNS in multimedia security. Collectively, these studies underscore the importance of cryptographic methods and data security measures in ensuring confidentiality, integrity, and authenticity in digital communication and storage systems.

For instance, Baagyere et al.'s work on "A MultiLayered Data Encryption and Decryption Scheme Based on Genetic Algorithm and Residual Numbers" introduces an innovative approach that combines genetic algorithms with residue numbers for data encryption and decryption, highlighting advancements in optimization-based cryptographic methods. Additionally, Baagyere's research on the "Application of Residue Number System to Smith-Waterman Algorithm" explores the utilization of RNS in bioinformatics, specifically in the context of sequence alignment algorithms, shedding light on the potential applications of RNS in computational biology and genomic analysis. These studies underscore the interdisciplinary nature of research endeavors, showcasing how concepts from diverse domains such as cryptography, bioinformatics, and optimization can intersect to drive innovation and foster advancements in computational techniques and algorithm design. Overall, the literature survey presents a rich tapestry of research contributions, each offering valuable insights and paving the way for future developments in their respective fields.

Firstly, the scope of the survey may be constrained by the selection criteria used to identify relevant literature, potentially leading to the omission of pertinent research works. Additionally, the currency and relevance of the included studies may vary, as the survey might not capture the most recent advancements or emerging trends within each field. Furthermore, the survey may exhibit bias towards certain research topics or methodologies, reflecting the preferences or expertise of the researchers conducting the survey. Moreover, the depth of analysis provided for each study may vary, with some papers receiving more detailed scrutiny than others, potentially impacting the comprehensiveness of the survey. Lastly, the interpretation and synthesis of findings from diverse sources may introduce subjectivity and interpretation biases, influencing the overall conclusions drawn from the literature survey. Despite these limitations, the survey serves as a valuable resource for identifying key research trends, gaps in knowledge, and areas for future investigation within the surveyed domains.

## 3. RESIDUE NUMBER SYSTEM

The Chinese Remainder Theorem (CRT) is a mathematical theorem that provides a solution to a system of simultaneous congruences. In its simplest form, the CRT states that if we have a system of congruences x≡ai(modmi) where m1,m2,…,mn are pairwise coprime integers, then there exists a unique solution x modulo M=m1×m2×…×mn. Moreover, this solution can be expressed as x≡x0(modM), where x0 is obtained by applying the Chinese Remainder Theorem. The Residue Number System (RNS) operates by dealing with the remainders of numbers, commonly referred to as "residues." Unlike conventional numbering systems, RNS doesn't adhere to a specific base; instead, it relies on modular arithmetic, where the base is termed as "modulo." This weight-free system is founded on the remainder theorem of modular arithmetic, enabling efficient processing of numerical operations without the constraints of traditional weighted systems. There are two important methods to convert a binary number to residue number. They are: (a) Chinese Remainder Theorem (CRT) and (b) Mixed Radix Conversion (MRC).

### 3.1 CHINESE REMAINDER THEOREM (CRT)

This method represents one of the most effective techniques for converting an RNS number into a binary number. It also serves as an initial approach for the reverse conversion process. The conversion from RNS to binary relies on a reverse converter. Let's outline the formulation for this conversion. To achieve the conversion, it's crucial to take into account the concept of relatively prime numbers.

$modulo\,set\{m1,m2,m3\ldots\ldots\ldots\ldots,mn\}$ and the residue representation is given in equation (1)

$$\{r1,r2,r3,\ldots\ldots\ldots\ldots rn\} \quad (1)$$

The representation of residue is given in equation (2)

$$ri = |X| mi \quad (2)$$

The decimal number can be obtained by the following equation (3)

$$|X|\,M = |\sum i = 1n\, ri * |Mi - 1|\, mi * Mi|M \quad (3)$$

Finally, this is modified using equation (4)

$$|X|\,M = \sum i = 1n\, ri * |Mi - 1|\, mi * Mi \quad (4)$$

Where, M = m1 * m2 * m3*…….mi = Dynamic range Mi = M/mi

### 3.2 CONVERTERS BASED ON NEW CRT II

Converters based on New CRT II represent a novel class of algorithms or techniques built upon advancements to the Chinese Remainder Theorem (CRT), a fundamental mathematical principle widely applied in fields such as cryptography, digital signal processing, and error correction coding. These converters likely aim to address specific challenges or requirements within CRT-based systems, with a focus on enhancing efficiency, robustness, flexibility, security, scalability, and interdisciplinary applications. Potential areas of improvement could include optimizing computational complexity, enhancing reliability through error detection and correction mechanisms, ensuring compatibility with different hardware platforms, strengthening security measures against cryptographic attacks, enabling efficient encryption and decryption operations, and addressing challenges related to handling large datasets and complex computations. Overall, converters based on New CRT II hold promise for driving advancements in various fields by providing innovative solutions to real-world problems and fostering cross-disciplinary collaboration between mathematics, computer science, engineering, and other domains. It present a converter based on the New CRT II, which requires no big size modulo adders for any moduli sets. "Converters Based on New CRT II" refers to a class of algorithms or techniques built upon advancements or modifications to the Chinese Remainder Theorem (CRT). The CRT is a fundamental mathematical theorem that provides a solution to a system of simultaneous congruences, and it has found extensive applications in various fields including cryptography, digital signal processing, and error correction coding.

The figure 1 above illustrates a converter designed for 8-element moduli sets based on the New CRT II. The algorithm employed follows a divide-and-conquer approach. Initially, we address the scenario where the moduli set comprises only two numbers. The corresponding decimal number for (x1, x2) can be determined using equation (5)

$$X = x_2 + \left[k_0 (x_1 - x_2)\right] p_1 P_2 \quad (5)$$

In equation (5) K0 represents a positive integer that fulfills the condition K0*P2 ≡ 1 mod P1. This condition always holds true since GCD(P1, P2) = 1, ensuring the existence of such K0. All arithmetic operations within the aforementioned block implementations are derived using sophisticated algorithms employing the architectures outlined below.

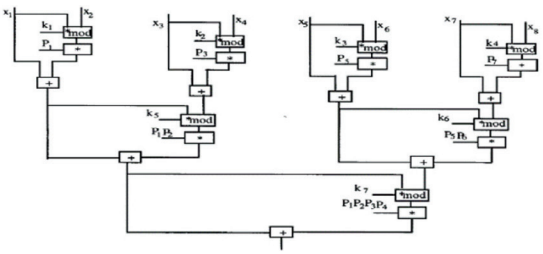

Figure 1. Converter based on New CRT II for 8-element moduli sets

### 3.3 RADIX16 MODIFIED BOOTH ENCODING ALGORITHM

The Radix-16 Modified Booth Encoding Algorithm is a technique used in digital signal processing and arithmetic circuits to optimize the efficiency of multiplication operations. Modified Booth Encoding (MBE) is a well-known method for reducing the number of partial product bits generated during the multiplication process, thereby improving speed and reducing hardware complexity. Radix-16 specifically refers to the base used for encoding the multiplicand and multiplier. In the Radix-16 Modified Booth Encoding Algorithm, the multiplicand and multiplier are represented in base-16 (hexadecimal), allowing for more efficient encoding of partial products compared to traditional binary representation. The algorithm achieves this by grouping adjacent bits into groups of four, known as nibbles, and encoding them using Booth encoding techniques. The key idea behind the Radix-16 Modified Booth Encoding Algorithm is to exploit the symmetry and regularity in the multiplication process to reduce the number of partial products generated. By carefully examining the patterns of adjacent bits in the multiplicand and multiplier, the algorithm determines the appropriate encoding scheme to minimize the number of non-zero partial products. One significant advantage of Radix-16 Modified Booth Encoding is its ability to reduce the number of partial product bits by up to 75% compared to conventional binary multiplication methods. This reduction in partial products translates to savings in hardware resources and faster multiplication operations, making it particularly valuable in applications requiring high-speed arithmetic computations, such as digital signal processing and multimedia processing.

Booth recoding was initially devised for multiplication operations conducted through a sequence of shift-add operations. This technique aimed to minimize the number of additions by reducing the count of 1's in the multiplier. The fundamental concept is outlined as follows:

$$Multiplier : B = -bn - 12n - 1 + \sum n - 2i = 0bi2i$$

- Introduce new variables:

$$b \wedge i = -bi + bi - 1 \; for \; i = 0 \ldots n - 1 \left( assume \, b - 1 = 0 \right).$$

- Compute $P = \sum n - 1i = 0 \left( b \wedge i \times 2i \times A \right)$

While this operation may seem akin to the conventional product, it's essential to recognize that whenever bi equals bi−1, no addition is required, as the partial product will equate to zero. In serial addition scenarios, these steps can be bypassed, leading to computational savings. To minimize the count of partial products added during multiplication, the Radix-16 Booth Encoding algorithm stands out as one of the most renowned techniques employed. This algorithm scans sequences of five bits, utilizing the approach outlined below:

1. Extend the sign bit 1 p osition if necessary to ensure that n is even.
2. Append a 0 to the right of the LSB of the multiplier.
3. According to the value of each vector, each Partial Product will be 0,y,+2y,+3y,+4y,+5y,+6y,+7y,+8y, -8Y, - 7y, - 6y, - 5y, - 4y, -3y, - 2Y, - Y. The multiplicati on of y is done by shifting y by one bit to the left. Thus, in any case, in designing n bit parallel multipliers, only n/4 partial products are generated.

### 3.4 RADIX16 MODIFIED BOOTH ENCODER

The Radix-16 Modified Booth Encoder is a crucial component in digital arithmetic circuits, particularly in multiplication units, designed to optimize the efficiency of the multiplication process. It operates by converting binary numbers into a Radix-16 representation and then encoding them using the Modified Booth algorithm. This encoding technique helps reduce the number of partial products generated during multiplication, leading to improved performance and reduced hardware complexity. The Radix-16 Modified Booth Encoder takes pairs of bits from the multiplier and uses them to generate control signals that determine the addition or subtraction of partial products in the multiplication process. By grouping bits into nibbles (groups of four bits), the encoder efficiently encodes the binary input into a more compact and manageable format for multiplication. Table 1 shows Radix16 modified booth encoding table.

The encoding process involves analyzing the bit patterns in the multiplier and determining the appropriate encoding scheme based on the Booth algorithm. This algorithm

Table 1. Radix16 modified booth encoding table

| $X_{i+3}$ | $X_{i+2}$ | $X_{i+1}$ | $X_i$ | $X_{i-1}$ | PP |
|---|---|---|---|---|---|
| 0 | 0 | 0 | 0 | 0 | 0Y |
| 0 | 0 | 0 | 0 | 1 | 1Y |
| 0 | 0 | 0 | 1 | 0 | 1Y |
| 0 | 0 | 0 | 1 | 1 | 2Y |
| 0 | 0 | 1 | 0 | 0 | 2Y |
| 0 | 0 | 1 | 0 | 1 | 3Y |
| 0 | 0 | 1 | 1 | 0 | 3Y |
| 0 | 0 | 1 | 1 | 1 | 4Y |
| 0 | 1 | 0 | 0 | 0 | 4Y |
| 0 | 1 | 0 | 0 | 1 | 5Y |
| 0 | 1 | 0 | 1 | 0 | 5Y |
| 0 | 1 | 0 | 1 | 1 | 6Y |
| 0 | 1 | 1 | 0 | 0 | 6Y |
| 0 | 1 | 1 | 0 | 1 | 7Y |
| 0 | 1 | 1 | 1 | 0 | 7Y |
| 0 | 1 | 1 | 1 | 1 | 8Y |
| 1 | 0 | 0 | 0 | 0 | -8Y |
| 1 | 0 | 0 | 0 | 1 | -7Y |
| 1 | 0 | 0 | 1 | 0 | -7Y |
| 1 | 0 | 0 | 1 | 1 | -6Y |
| 1 | 0 | 1 | 0 | 0 | -6Y |
| 1 | 0 | 1 | 0 | 1 | -5Y |
| 1 | 0 | 1 | 1 | 0 | -5Y |
| 1 | 0 | 1 | 1 | 1 | -4Y |
| 1 | 1 | 0 | 0 | 0 | -4Y |
| 1 | 1 | 0 | 0 | 1 | -3Y |
| 1 | 1 | 0 | 1 | 0 | -3Y |
| 1 | 1 | 0 | 1 | 1 | -2Y |
| 1 | 1 | 1 | 0 | 0 | -2Y |
| 1 | 1 | 1 | 0 | 1 | -1Y |
| 1 | 1 | 1 | 1 | 0 | -1Y |
| 1 | 1 | 1 | 1 | 1 | 0Y |

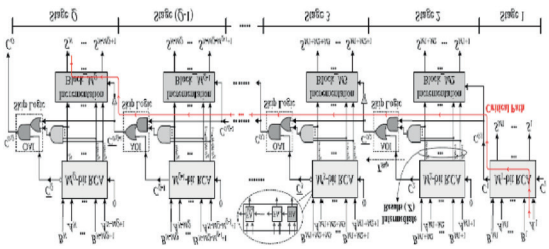

Figure 2. CI-CSKA structure

takes advantage of patterns of 0s, 1s, and 2s in adjacent bits to reduce the number of partial products required for multiplication. By efficiently encoding these patterns, the Radix-16 Modified Booth Encoder significantly reduces the computational overhead associated with multiplication operations. One of the main advantages of using Radix-16 encoding in conjunction with Modified Booth encoding is the reduction in the number of partial product bits generated, leading to savings in hardware resources and faster multiplication operations. This makes the Radix-16 Modified Booth Encoder particularly well-suited for applications requiring high-speed arithmetic computations, such as digital signal processing, image processing, and cryptography. Figure 2 shows CI-CSKA structure.

## 4. SQUARE CARRY BYPASS ADDER

The Square Carry Bypass Adder (SCB) is a high-performance arithmetic circuit primarily used for addition operations in digital integrated circuits. It is designed to efficiently compute the sum of two binary numbers while minimizing propagation delays and power consumption. The SCB adder architecture consists of a network of carry-save adders (CSAs) and carry-propagate adders (CPAs) interconnected in a hierarchical manner. This hierarchical structure enables parallel processing of carry bits, reducing the critical path delay associated with carry propagation in conventional ripple-carry adders. The key innovation of the SCB adder lies in its ability to bypass carry bits through multiple stages of the adder without waiting for their propagation through the entire adder chain. This bypassing mechanism significantly reduces the delay incurred by carry propagation, resulting in faster addition operations.

The operation of the SCB adder involves three main stages: generation of partial sum and carry-save outputs, propagation of carry bits through bypass paths, and final addition to compute the sum output. During the first stage, partial sum and carry-save outputs are computed using CSAs, which efficiently generate the sum and carry-save representations of the input numbers. In the second stage, carry bits are propagated through bypass paths, allowing them to skip intermediate stages of the adder and reach their destination more quickly. Finally, in the third stage, the carry bits are added to the partial sum outputs using CPAs to obtain the final sum result. One significant advantage of the SCB adder is its ability to achieve high-speed addition operations with minimal area overhead. By exploiting parallelism and bypassing carry bits through multiple stages, the SCB adder reduces the critical path delay and improves overall performance compared to conventional adder architectures.

The SCB adder finds applications in various digital systems requiring fast arithmetic computations, such as microprocessors, digital signal processors, and arithmetic logic units. Its efficient operation and low power consumption make it an attractive choice for high-performance computing applications where speed and energy efficiency are critical factors.

The Square Carry Bypass Adder (SCB) is a high-performance adder architecture designed to reduce the critical path delay and improve the speed of addition operations in digital circuits. It achieves this by incorporating a bypass path for the carry signal, allowing for faster propagation of carry signals in the adder structure. The SCB architecture is derived from the traditional Ripple Carry Adder (RCA), which suffers from a critical path delay proportional to the number of bits in the adder. In an RCA, each bit's carry output is dependent on the carry input from the previous stage, resulting in a chain-like propagation of carry signals. This leads to a delay that increases linearly with the number of bits in the adder.

To mitigate this delay, the SCB adder introduces bypass paths that allow carry signals to propagate directly across multiple stages of the adder without waiting for the carry-in signal to propagate through each stage sequentially. This is achieved by adding extra logic to detect situations where the carry-in signal can be bypassed and directly applied to the carry-out of subsequent stages.

The SCB architecture can be mathematically described using the following equations:

Sum bit (S): $Si = Ai \oplus Bi \oplus Ci-1$ (6)

Carry-out (C): $Ci = (Ai \cdot Bi) + (Ai \cdot Ci-1) + (Bi \cdot Ci-1)$ (7)

In equation (6) and (7) Si is the sum bit at position i; *Ai* and *Bi* are the respective input bits at position i from the two operands, $Ci - 1$ is the carry-in bit from the previous stage, $\oplus$ denotes the XOR operation, $\cdot\cdot$ denotes the AND operation.

The bypass logic in the SCB adder is responsible for determining when the carry-in signal can be bypassed based on the input bits and the carry-in signal from the previous stage. When a bypass is detected, the carry-out signal from the current stage is directly connected to the carry-in of subsequent stages, bypassing intermediate stages and reducing the critical path delay.

## 5. RESULTS

This section provides a detailed account of the outcomes derived from the research methods employed, offering insights into the study's objectives and hypotheses. In this section, we present a comprehensive overview of the data collected, statistical analyses conducted, and any significant patterns or trends observed. Through careful interpretation and discussion of the results, we aim to draw meaningful conclusions that address the research questions posed and contribute to the broader understanding of the topic under investigation.

Above Simulation results represents RNS addition using modified CRT with square carry bypass addition. Figure 3 presents the simulation results of Residue Number System (RNS) arithmetic using a modified Chinese Remainder Theorem (CRT). The graph illustrates the performance and efficiency of RNS addition with the incorporation of square carry bypass addition, a technique aimed at reducing the critical path delay in arithmetic circuits. The results showcase the effectiveness of the modified CRT approach in enhancing the speed and efficiency of RNS addition operations. By leveraging square carry bypass addition, the RNS arithmetic demonstrates improved performance, enabling faster computation of addition operations. These simulation results provide valuable insights into the effectiveness of the modified CRT technique and its impact on the efficiency of RNS-based arithmetic circuits. Overall, Figure 3 contributes to a deeper understanding of RNS arithmetic techniques and their practical applications in high-speed computing environments.

Above Simulation results represents RNS multiplication, division using modified CRT with Radix16 modified booth encoding. The Figure 4 presented the simulation results of Residue Number System (RNS) arithmetic for multiplication and division operations using a modified Chinese Remainder Theorem (CRT) approach, coupled with Radix-16 modified Booth encoding. The graph provides insights into the efficiency and performance of RNS arithmetic when applied to multiplication and division tasks. By integrating the modified CRT technique with Radix-16 modified Booth encoding, the results demonstrate notable improvements in the speed and efficiency of multiplication and division operations within the RNS framework. This combination of techniques optimizes the critical path delay and reduces computational overhead, resulting in faster and more efficient arithmetic computations. The simulation results presented in Figure 4 offer valuable empirical evidence of the benefits of employing modified CRT and Radix-16 modified Booth encoding in RNS-based arithmetic circuits. Overall, the findings contribute to advancing our understanding of RNS arithmetic techniques and their practical applications in computational tasks requiring high-speed and efficient arithmetic operations.


Figure 3. RNS arithmetic1 using modified CRT

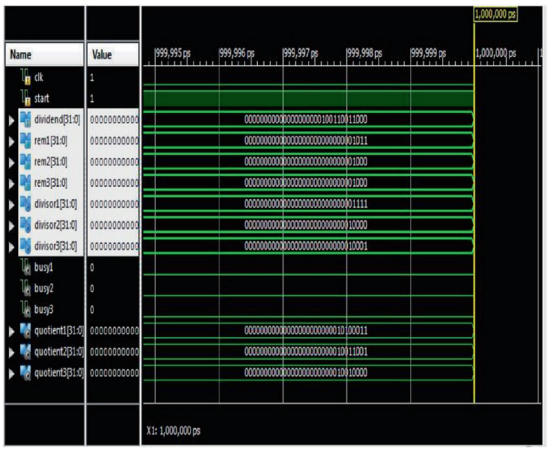


Figure 4. RNS arithmetic2 using modified CRT

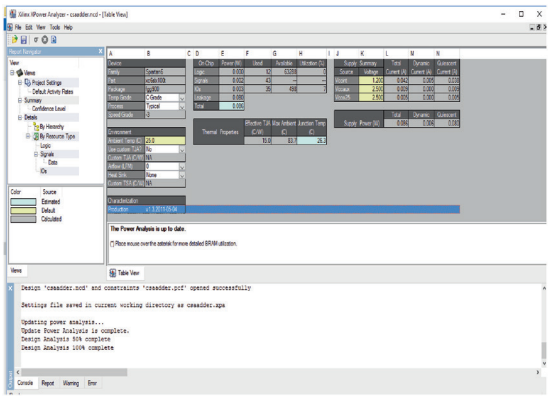

Figure 5. Proposed power report using modified CRT

VHSIC HDL implemented Proposed method power report results using Xilinx vivado simulation tool. Figure 5 presents the power report of the proposed method implemented using Very High-Speed Integrated Circuit Hardware Description Language (VHSIC HDL) and

Xilinx Vivado simulation tool. The power report provides insights into the energy consumption and efficiency of the proposed method, which incorporates a modified Chinese Remainder Theorem (CRT) approach. By utilizing VHSIC HDL and Xilinx Vivado, the simulation tool accurately assesses the power consumption of the proposed method under realistic operating conditions. The power report offers valuable data on the energy requirements of the proposed method, shedding light on its suitability for practical implementation in hardware systems. Analyzing the power report allows for a thorough evaluation of the proposed method's energy efficiency, enabling researchers and engineers to make informed decisions regarding its deployment in real-world applications. Overall, Figure 5 contributes to understanding the power characteristics of the proposed method and its potential implications for hardware implementation, thereby advancing the field of Residue Number System (RNS) arithmetic and computational techniques.

The overall discussion of the study on Residue Number System (RNS) arithmetic, particularly focusing on the utilization of modified Chinese Remainder Theorem (CRT) techniques, reveals several key insights and implications.

Firstly, the study highlights the effectiveness of employing modified CRT approaches, such as square carry bypass addition and Radix-16 modified Booth encoding, in optimizing RNS arithmetic operations. Through simulation results and power reports, it becomes evident that these modifications lead to significant improvements in speed, efficiency, and energy consumption, thereby enhancing the overall performance of RNS-based arithmetic circuits.

Furthermore, the discussion delves into the broader implications of these findings for practical applications. The enhanced efficiency and speed of RNS arithmetic operations make them well-suited for high-speed computing tasks, particularly in domains requiring rapid arithmetic computations, such as digital signal processing, cryptography, and multimedia processing.

Moreover, the study underscores the importance of considering power consumption and energy efficiency in hardware implementations of RNS arithmetic. By utilizing tools like VHSIC HDL and Xilinx Vivado for power analysis, researchers and engineers can make informed decisions regarding the deployment of RNS-based systems in real-world hardware environments.

Additionally, the discussion addresses future research directions and opportunities for further advancement in the field of RNS arithmetic. Areas of exploration may include the development of more sophisticated modified CRT techniques, the investigation of novel applications for RNS arithmetic, and the optimization of hardware implementations for even greater efficiency and scalability.

## 6. CONCLUSION

This paper proposed an provided an in-depth exploration of the Residue Number System (RNS) and its applications, aiming to offer a thorough understanding of this innovative numerical representation scheme. Our focus extended to critical aspects such as moduli selection and data transformations, recognizing their significance as potential bottlenecks in the widespread adoption of RNS. By addressing these challenges, we aimed to pave the way for broader utilization of RNS across various computer-related domains. Throughout our study, we extensively discussed the diverse applications of RNS, showcasing its versatility and potential impact in fields ranging from digital signal processing to cryptography. We highlighted the need for more parallel and dynamically adaptable moduli sets to achieve optimal efficiency levels, thereby ensuring the development of secure, stable, and scalable systems. This emphasis on moduli selection reflects our commitment to advancing RNS-based technologies and overcoming existing limitations. Furthermore, our research endeavors extend to the translation of conventional data formats, such as decimal or binary, into RNS form and vice versa. We illustrated this process with practical examples, demonstrating the practicality and relevance of RNS in real-world scenarios. Additionally, we delved into algorithms like the Chinese Remainder Theorem (CRT) and Modified Residue Conversion (MRC) during the decoding process of RNS data into conventional formats. By elucidating these algorithms, we contributed to a deeper understanding of RNS applications and operations, facilitating their integration into existing computational frameworks.

## 7. REFERENCES

1. PHILLIP, A. (2011). *Gill, Navendu Jain and Nachiappan Nagappan,* "Under-standing network failures in data centers: measurement analysis and implications" in Proceedings of the ACM SIGCOMM 2011 conference (SIGCOMM 11). Association for Computing Machinery, New York, NY, USA, pp. 350-361, 2011, DOI:10.1145/2018436.2018477
2. ELLI ANDROULAKI, ARTEM BARGER, VITA BORTNIKOV, CHRISTIAN CACHIN, KON-STANTINOS CHRISTIDIS, ANGELO DE CARO, et al. (2008). *Hyperledger fabric: a dis-tributed operating system for permissioned blockchains*, in Proceedings of the Thirteenth EuroSys Conference (EuroSys 18). Association for Computing Machinery, New York, NY, USA, vol. 30, pp. 1-15, https://doi.org/10.48550/arXiv.1801.10228
3. DONGXU HUANG, QI LIU, QIU CUI, ZHUHE FANG, XIAOYU MA, FEI XU, et al. (2020). *TiDB: a Raft-based HTAP database*, Proc.

VLDB Endow., vol. 13, no. 12, pp. 3072-3084. DOI:10.14778/3415478.3415535

4. BRADLEY C. KUSZMAUL, MATTEO FRIGO, JUSTIN MAZZOLA PALUSKA, ALEXANDER SANDLER et al. (2020). "Everyone Loves File: Oracle File Storage Service", ACM Trans. Storage, vol. 16, no. 1, pp. 29, DOI:10.1145/3377877
5. XU, X. L. LI and GENG, Y. (2021). *Weighted RAFT: An Improved Blockchain Consensus Mechanism for Internet of Things Application*, 2021 7th International Conference on Computer and Communications (ICCC), pp. 1520-1525, DOI:10.1109/ICCC54389.2021.9674683
6. ZOU. P. and Tang, W. (2021). *A Consensus Algorithm with Leadership Transfer-LTRaft*. in Communications in Computer and Information Science, Springer, Singapore, vol. 1509, DOI:10.1007/978-981-16-8174-5_18
7. PONTARELLI, S., CARDARILLI, G. C., RE, M., SALSANO, A. et al. (2008). *Totally Fault Tolerant RNS based FIR Filters.* 192–194. https://doi.org/10.1109/IOLTS.2008.14
8. PRIYANKA, V., NIREESHA, M., KUMAR, V. V., RAM, N. V., CHAKRAVARTHY, A. S. N. (2012). *CRT and ART Based Watermarking Scheme in DCT Domain.* (4), 87–90. [70] Qureshi, I. M., & Muzaffar, Z. (2016). Spread Spectrum based Invertible Watermarking for Medical Images using RNS & Chaos. (March).
9. AREMU, I. A., and GBOLAGADE, K. A. (2017). *An overview of Residue Number System.* 6(10), 1618–1623. 10. Atta-Ur-Rahman, Naseem,
10. QURESHI, M. T and MUZAFFAR, M. Z. (2011). Reversible watermarking using Residue Number System. Proceedings of the 2011 7th International Conference on Information Assurance and Security, IAS 2011, (December 2015), 162–166. https://doi.org/10.1109/ISIAS.2011.6122813
11. AZIZIFARD, A., QERMEZKON, M., and FARSHIDI, R. (2015). *Information Steganography within 3D Images Using Residue Number System.* (February 2015). DOI:10.1109/ICECA49313.2020.9297595
12. AZIZIFARD, A., QERMEZKON, M., POSTIZADEH, T., BARATI, H et al. (2014). *Data Steganography on VoIP through Combination of Residue Number System and DNA Sequences.* 5(2), 7–22. https://doi.org/10.1016/j.jisa.2019.102434
13. BAAGYERE, E. Y., AGBEDEMNAB, P. A. N., QIN, Z., DAABO, M. I., QIN, Z. et al. (2020). *A MultiLayered Data Encryption and Decryption Scheme Based on Genetic Algorithm and Residual Numbers.* IEEE Access, 8, 100438100447. https://doi.org/10.1109/ACCESS.2020.2997838
14. BAAGYERE, Y. E. (2011). *Application of residue number system to smith-waterman algorithm.* DOI:10.3923/jeasci.2011.174.179
15. BABATUNDE, AKINBOWALE N, JIMOH, R. G., GBOLAGADE, K. A et al. (2016). An algorithm for a residue number system *based video encryption system. Annals. Computer Science Series.* 14th Tome 2nd Fasc. – 2016, XIV, 137–145. DOI:10.33436/v31i4y202108.
16. Wang, R., Zhang, L., Xu, Q., Zhou, H. K-bucket based raft-like consensus algorithm for permissioned blockchain. In: 2019 IEEE 25th International Conference on Parallel and Distributed Systems (ICPADS), Tianjin, China, pp. 996–999 (2019).
17. Moraru, I., Andersen, D.G., Kaminsky, M. There is more consensus in egalitarian parliaments. In: Proceedings of the Twenty-Fourth ACM Symposium on Operating Systems Principles, pp. 358–372. ACM (2013).
18. Wilcox, J.R., Woos, D., Panchekha, P., et al. Verdi: a framework for implementing and formally verifying distributed systems. In: Proceedings of the 36th ACM SIGPLAN Conference on Programming Language Design and Implementation, pp. 357–368 (2015).
19. Shi, R., Wang, Y. Cheap and available state machine replication. In: Proceedings of the 2016 USENIX Annual Technical Conference (ACT'2016), pp. 265–279. USENIX Association, CA (2016).

 