2012

Design of reverse converters for the multi-moduli residue number systems with moduli of forms 2a, 2b - 1, 2c + 1

Naveen Kumar Samala
Louisiana State University and Agricultural and Mechanical College

DESIGN OF REVERSE CONVERTERS FOR THE MULTI-MODULI RESIDUE NUMBER SYSTEMS WITH MODULI OF FORMS $2^a, 2^b - 1, 2^c + 1$

A Thesis

Submitted to the Graduate Faculty of the
Louisiana State University and
Agricultural and Mechanical College
in partial fulfillment of the
requirements for the degree of
Master of Science in Electrical Engineering

in

The Department of Electrical Engineering and Computer Engineering

by
Naveen Kumar Samala
Bachelor of Engineering (Electrical and Electronics)
Osmania University, 2008
May 2012

ACKNOWLEDGEMENTS

First and foremost I would like to offer my sincerest gratitude to my advisor, Dr. Alexander Skavantzos, for his constant support and guidance throughout my research with his patience and knowledge. I attribute the level of my Master's degree to his encouragement and effort and without him this thesis, too, would not have been completed or written. I am indebted to him more than he knows.

I am also grateful to Dr. Suresh Rai and Dr. Ashok Srivastava for accepting my request and being a part of my thesis committee.

I would like to thank Mark Hovey for providing financial assistance for the second academic year of my Masters studies at LSU. I enjoyed working with him and gained professional experience, which will be helpful to me to start my professional career at United States. I would also express my gratitude to Dr. Svetlana Oard for providing financial support during my first year of my Masters. I enhanced my skills in research, computer programming and documenting research by working with her.

Finally, it gives me immense pleasure to acknowledge my parents- Vijaya Laxmi Samala and Ram Prakash Samala, my brother Girish Kumar Samala, my sister Ambica Ambati, my brother-in-law Ravinder Ambati, relatives and all my friends who have helped me in making this thesis a successful one. Special thanks to my cousins Rama Devi Goshika and Vijay Kumar Goshika.

TABLE OF CONTENTS

LIST OF TABLES

Table **Page**

LIST OF FIGURES

Figure **Page**

ABSTRACT

Residue number system (RNS) is a non-weighted integer number representation system that is capable of supporting parallel, carry-free and high speed arithmetic. This system is error-resilient and facilitates error detection, error correction and fault tolerance in digital systems. It finds applications in Digital Signal Processing (DSP) intensive computations like digital filtering, convolution, correlation, Discrete Fourier Transform, Fast Fourier Transform, etc.

The basis for an RNS system is a moduli set consisting of relatively prime integers. Proper selection of this moduli set plays a significant role in RNS design because the speed of internal RNS arithmetic circuits as well as the speed and complexity of the residue to binary converter (R/B or Reverse Converter) have a large dependency on the form and number of the selected moduli. Moduli of forms 2^a, $2^b - 1$, $2^c + 1$ (a, b and c are natural numbers) have the most use in RNS moduli sets as these moduli can be efficiently implemented using usual binary hardware that lead to simple design. Another important consideration for the reverse converter design is the selection of an appropriate conversion algorithm from Chinese Remainder Theorem (CRT), Mixed Radix Conversion (MRC) and the new Chinese Remainder Theorems (New CRT I and New CRT II).

This research is focused on designing reverse converters for the multi-moduli RNS sets especially four and five moduli sets with moduli of forms 2^a, $2^b - 1$, $2^c + 1$. The residue to binary converters are designed by applying the above conversion algorithms in different possible ways and facilitating the use of modulo (2^k) and modulo ($2^k - 1$) adders that lead to simple design of adder based architectures and VLSI efficient implementations (k is a natural number). The area and delay of the proposed converters is analyzed and an efficient reverse converter is suggested from each of the various four and five moduli set converters for a given dynamic range.

1. INTRODUCTION TO RESIDUE NUMBER SYSTEMS

1.1 Introduction:

Residue number system (RNS) is a non-weighted integer number representation system and uses residues of a number in particular modulus for its representation [1], [2]. It is capable of supporting parallel, carry-free and high speed arithmetic. One of the most important characteristics of the RNS is the limited propagation of the carry-out digit among modulus in arithmetic. Instead of performing arithmetic on a large number, calculations are done in parallel on its corresponding residues. This feature significantly increases the calculation speed and decreases the consumed power. Considering the characteristics of the RNS, this system has been applied on many arithmetic applications such as Digital Signal Processing (DSP) intensive computations like digital filtering, convolutions, correlations, Discrete Fourier Transform (DFT) computations, Fast Fourier Transform (FFT) computations and direct digital frequency synthesis [3]-[7]. Moreover, RNS has applications in image processing systems, especially RNS image coding which can offer high speed VLSI implementation of secure image processing algorithms [8]. In addition, RNS architectures are essentially error-resilient and facilitate error detection, error correction and fault tolerance in digital systems [9], [10].

1.2 Basics of Residue Number System:

The Residue Number System is defined in terms of relatively-prime integer moduli set

$$S = \{m_1,\ m_2, \ldots., m_L\}, \text{ where } \gcd(m_i,\ m_j) = 1 \ \text{ for } i \neq j \qquad (1.1)$$

with $\gcd(m_i,\ m_j)$ indicating the greatest common divisor of m_i and m_j.

1.2.1 Weighted to RNS conversion:

A weighted number X can be represented in RNS as

$$X \xrightarrow{RNS} (x_1, x_2, \dots, x_L) \tag{1.2}$$

where

$$x_i = X \bmod m_i = |X|_{m_i}, 0 \leq x_i < m_i, i = 1, 2, \dots, \text{L} \tag{1.3}$$

Such a representation is unique for any integer X in the range [0, M - *1*], where M is the dynamic range of the system defined by the product of all moduli m_i in the set *S*. The equations (1.2) and (1.3) shows the weighted to RNS conversion of number X. The integers x_i are called residues.

1.2.2 Arithmetic Operations on RNS Numbers:

If the integers X and Y have RNS representations as

$$X \xrightarrow{RNS} (x_1, x_2, \dots, x_L) \tag{1.4}$$

$$Y \xrightarrow{RNS} (y_1, y_2, \dots, y_L) \tag{1.5}$$

then the RNS representation of W is given by

$$W = X \oplus Y \xrightarrow{RNS} (|x_1 \oplus y_1|_{m_1}, |x_2 \oplus y_2|_{m_2}, \dots, |x_L \oplus y_L|_{m_L}) \tag{1.6}$$

where $\oplus$ denotes addition, subtraction, or multiplication. Equation (1.6) demonstrates that the arithmetic operations in RNS domain are parallel and carry-free.

1.2.3 Dynamic Range of RNS:

Let M be the product of all the moduli m_i in the moduli set *S*. For unsigned number representation of RNS system, the dynamic range is

$$DR = [0, M-1] \tag{1.7}$$

If the RNS system supports signed numbers then the dynamic range is

$$DR = \left[-\frac{M}{2}, \left(\frac{M}{2}\right) - 1\right], \text{ if M is even} \tag{1.8}$$

$$DR = \left[-\frac{M-1}{2}, \frac{M-1}{2}\right], \text{ if M is odd} \tag{1.9}$$

1.2.4 RNS to Weighted Conversion:

The residue to binary (R/B or Reverse) conversion is mainly based on the following reverse conversion algorithms:

1) Chinese Remainder Theorem (CRT)

2) Mixed Radix Conversion (MRC)

3) New Chinese Remainder Theorem 1 (New CRT-I)

4) New Chinese Remainder Theorem 2 (New CRT-II)

1.2.4.1 Chinese Remainder Theorem (CRT):

Let the RNS representation of an integer X be $(x_1, x_2, \dots, x_L)$ using the moduli set $S = \{m_1,\ m_2, \dots, m_L\}$, $\gcd(m_i,\ m_j) = 1$ for $i \neq j$. The number X can be constructed from its residue representation x_i by CRT [1], [2] as follows:

$$X = |x_1 M_1 N_1 + x_2 M_2 N_2 \dots\dots + x_L M_L N_L|_M = |\sum_{i=1}^{L} X_i M_i N_i|_M \tag{1.10}$$

Alternately, we can have

$$X = ||x_1 N_1|_{m_1} M_1 + |x_2 N_2|_{m_2} M_2 \dots\dots + |x_L N_L|_{m_3} M_L|_M = |\sum_{i=1}^{L} |X_i N_i|_{m_i} M_i|_M \tag{1.11}$$

where

$$M = \prod_{i=1}^{L} m_i \tag{1.12}$$

$$M_i = \frac{M}{m_i} \text{ and } N_i = |M_i^{-1}|_{m_i} \quad (1.13)$$

Here, $|M_i^{-1}|_{m_i}$ is the multiplicative inverse of M_i modulo m_i.

For a three moduli set $\{m_1, m_2, m_3\}$, $\gcd(m_i, m_j) = 1$ for $i \neq j$, the number X can be converted from its corresponding residues (x_1, x_2, x_3) by CRT as follows:

$$X = |x_1 M_1 N_1 + x_2 M_2 N_2 + x_3 M_3 N_3|_M = | \, |x_1 N_1|_{m_1} M_1 + |x_2 N_2|_{m_2} M_2 + |x_3 N_3|_{m_3} M_3|_M \quad (1.14)$$

where

$$M_1 = \frac{M}{m_1}, M_2 = \frac{M}{m_2}, M_3 = \frac{M}{m_3}, \; N_1 = |M_1^{-1}|_{m_1}, N_2 = |M_2^{-1}|_{m_2}, N_3 = |M_3^{-1}|_{m_3} \quad (1.15)$$

1.2.4.2 Mixed Radix Conversion (MRC):

Let the RNS representation of an integer X be $(x_1, x_2, \ldots, x_L)$ using the moduli set $S = \{m_1, m_2, \ldots, m_L\}$, $\gcd(m_i, m_j) = 1$ for $i \neq j$. The number X can be constructed from its residue representation x_i by MRC [1], [2] as follows:

$$X = x_1' + m_1 x_2' + m_1 m_2 x_3' + m_1 m_2 m_3 x_4' + \ldots + m_1 m_2 m_3 m_4 \ldots m_{L-1} x_L' \quad (1.16)$$

where $x_1', x_2', x_3', x_4', \ldots, x_L'$ are called the mixed radix digits and x_i' belongs to $Z_{m_i} = [0, m_i - 1]$. The mixed radix digits $x_1', x_2', x_3', x_4', \ldots, x_L'$ can be represented as functions of the residues $x_1, x_2, x_3, x_4, \ldots, x_L$ and the moduli $\{m_1, m_2, \ldots, m_L\}$. These mixed radix digits have respective weights associated with them. The weight associated with x_1' is 1, x_2' is m_1, x_3' is $m_1 m_2$, and similarly the weight associated with x_L' is $m_1 m_2 m_3 m_4 \ldots m_{L-1}$.

For a two moduli set $\{m_1, m_2\}$, $\gcd(m_1, m_2) = 1$, the integer X can be constructed from its residue representation (x_1, x_2) by MRC as follows:

$$X = x_1 + m_1 \cdot | \, |m_1^{-1}|_{m_2} \cdot (x_2 - x_1) \, |_{m_2} \quad (1.17)$$

1.2.4.3 New Chinese Remainder Theorem 1 (New CRT I):

Let the RNS representation of an integer X be $(x_1, x_2, \dots, x_L)$ using the moduli set $S = \{m_1,\ m_2, \dots., m_L\}$, $\gcd(m_i,\ m_j) = 1$ for $i \neq j$. The number X can be constructed from its residue representation x_i by New CRT I [11], [12], [13] as follows:

$$X = x_1 + m_1 |\, k_1(x_2 - x_1) + k_2 m_2(x_3 - x_2) + \cdots + k_{L-1} m_1 \cdots m_{L-1}(x_L - x_{L-1})|_{m_2 \cdots m_{L-1} m_L} \tag{1.18}$$

where

$$k_1 = |m_1^{-1}|_{m_2 \cdots m_L},\ k_2 = |(m_1 m_2)^{-1}|_{m_3 \cdots m_L}, \dots.., k_{L-1} = |(m_1 m_2 \cdots m_{L-1})^{-1}|_{m_L} \tag{1.19}$$

For a three moduli set $\{m_1,\ m_2,\ m_3\}$, the binary number X can be calculated by New CRT I as

$$X = x_1 + m_1 |\, k_1(x_2 - x_1) + k_2 m_2(x_3 - x_2)|_{m_2 m_3} \tag{1.20}$$

where

$$k_1 = |m_1^{-1}|_{m_2 m_3}, \text{ and } k_2 = |(m_1 m_2)^{-1}|_{m_3} \tag{1.21}$$

For a four moduli set $\{m_1,\ m_2,\ m_3,\ m_4\}$, the binary number X can be calculated by New CRT I as

$$X = x_1 + m_1 |\, k_1(x_2 - x_1) + k_2 m_2(x_3 - x_2) + k_3 m_2 m_3(x_4 - x_3)|_{m_2 m_3 m_4} \tag{1.22}$$

where

$$k_1 = |m_1^{-1}|_{m_2 m_3 m_4},\ k_2 = |(m_1 m_2)^{-1}|_{m_3 m_4} \text{ and } k_3 = |(m_1 m_2 m_3)^{-1}|_{m_4} \tag{1.23}$$

For a five moduli set $\{m_1,\ m_2,\ m_3,\ m_4,\ m_5\}$, the binary number X can be calculated by New CRT I as

$$X = x_1 + m_1 |\, k_1(x_2 - x_1) +$$

$$k_2 m_2(x_3 - x_2) + k_3 m_2 m_3(x_4 - x_3) + k_4 m_2 m_3 m_4(x_5 - x_4)|_{m_2 m_3 m_4 m_5} \tag{1.24}$$

where

$$k_1 = |m_1^{-1}|_{m_2 m_3 m_4 m_5}, k_2 = |(m_1 m_2)^{-1}|_{m_3 m_4 m_5}, k_3 = |(m_1 m_2 m_3)^{-1}|_{m_4 m_5} \text{and}$$

$$k_4 = |(m_1 m_2 m_3 m_4)^{-1}|_{m_5} \tag{1.25}$$

For a six moduli set $\{m_1,\ m_2,\ m_3,\ m_4,\ m_5,\ m_6\}$, the binary number *X* can be calculated by New CRT I as

$$X = x_1 + m_1 | k_1(x_2 - x_1) + k_2 m_2(x_3 - x_2) + k_3 m_2 m_3(x_4 - x_3) +$$

$$k_4 m_2 m_3 m_4(x_5 - x_4) + k_5 m_2 m_3 m_4 m_5(x_6 - x_5)|_{m_2 m_3 m_4 m_5 m_6} \tag{1.26}$$

where

$$k_1 = |m_1^{-1}|_{m_2 m_3 m_4 m_5 m_6}, k_2 = |(m_1 m_2)^{-1}|_{m_3 m_4 m_5 m_6}, k_3 = |(m_1 m_2 m_3)^{-1}|_{m_4 m_5 m_6}$$

$$k_4 = |(m_1 m_2 m_3 m_4)^{-1}|_{m_5 m_6} \text{and } k_5 = |(m_1 m_2 m_3 m_4 m_5)^{-1}|_{m_6} \tag{1.27}$$

1.2.4.4 New Chinese Remainder Theorem 2 (New CRT II):

Let the RNS representation of an integer *X* be (x_1, x_2, x_3, x_4) using the four moduli set $S = \{m_1, m_2, m_3, m_4\}$, $\gcd(m_i,\ m_j) = 1$ for $i \neq j$. The number *X* can be constructed from its residue representation x_i by New CRT II [11], [12], [14] as follows:

$$X = Z + m_1 m_2 | k_1(Y - Z)|_{m_3 m_4} \tag{1.28}$$

where

$$Z = x_1 + m_1 \mid k_2(x_2 - x_1) \mid_{m_2} \tag{1.29}$$

$$Y = x_3 + m_3 \mid k_3(x_4 - x_3) \mid_{m_4} \tag{1.30}$$

$$k_1 = |(m_1 m_2)^{-1}|_{m_3 m_4}, k_2 = |m_1^{-1}|_{m_2} \text{ and } k_3 = |m_3^{-1}|_{m_4} \tag{1.31}$$

1.3 Modular Arithmetic:

1.3.1 Properties of Modulo m Operator:

Addition/Subtraction modulo m

- $| x \pm y |_m = | |x|_m \pm |y|_m |_m$ (1.32)

  Example: $| 17 \pm 19 |_7 = | |17|_7 \pm |19|_7 |_7 = | 3 + 5 |_7 = | 8 |_7 = 1$

  Multiplication modulo m

- $| x \cdot y |_m = | |x|_m \cdot |y|_m |_m$ (1.33)

  Example: $| 12 \cdot 11 |_7 = | |12|_7 \cdot |11|_7 |_7 = | 5 \cdot 4 |_7 = | 20 |_7 = 6$

  Additive Inverse modulo m

- $|-a |_m = | m - a |_m$ (1.34)

  Example: $|-12 |_{15} = | 15 - 12 |_{15} = |3 |_{15} = 3$

  Multiplicative Inverse modulo m

- $|a^{-1} |_m = b \; ; \; b \in \{1, 2, \dots, m-1\}$ (1.35)

  where b is such that $| a \cdot b |_m = 1$

  $|a^{-1} |_m$ exists if and only if a and m are relatively prime

  Example: $|5^{-1} |_{11} = 9$

1.3.2 Properties of Arithmetic Modulo $(2^n - 1)$ Operator:

Let *A*, *B* be integers such that $A \in Z_{2^n-1}$, $B \in Z_{2^n-1}$, where $Z_{2^n-1} = [0, 2^n - 2]$.

Property 1: The residue of addition of residue numbers *A* and *B* in modulo $2^n - 1$ is 1's complement addition of *A* and *B*, i.e., addition of *A* and *B* and end around carry.

$|A + B|_{2^n-1}$ = 1's complement addition of *A* and *B* (1.36)

Property 2: The residue of subtraction of residue numbers A and B in modulo $2^n - 1$ is 1's complement addition of A and $\bar{B}$, i.e., addition of A and $\bar{B}$ and end around carry, where $\bar{B}$ is 1's complement of B.

$$|A - B|_{2^n-1} = \text{1's complement addition of } A \text{ and } \bar{B} \tag{1.37}$$

Property 3: The residue of a negative residue number $(-A)$ in modulo $(2^n - 1)$ is the 1's complement of A.

$$|-A|_{2^n-1} = \text{1's complement of } A \tag{1.38}$$

Property 4: The multiplication of a residue number A by 2^p in modulo $(2^n - 1)$ is carried out by p bit circular left shift, where p is a natural number.

$$|2^p \cdot A|_{2^n-1} = \text{CLS(A, p)} \tag{1.39}$$

where the function CLS(x, r) is used to denote a circular shift of the binary number x by r bits to the left.

1.3.3 Properties of Arithmetic Modulo (2^n) Operator:

Let A, B be integers such that $A \in Z_{2^n}$, $B \in Z_{2^n}$, where $Z_{2^n} = [0, 2^n - 1]$.

Property 1: The residue of addition of residue numbers A and B in modulo 2^n is 2's complement addition of A and B, i.e., addition of A and B and ignoring carry out.

$$|A + B|_{2^n} = \text{2's complement addition of } A \text{ and } B \tag{1.40}$$

Property 2: The residue of subtraction of residue numbers A and B in modulo 2^n is 2's complement addition of A and B', i.e., addition of A and B' and ignoring carry out, where B' is 2's complement of B.

$$|A - B|_{2^n} = \text{2's complement addition of } A \text{ and } B' \tag{1.41}$$

Property 3: The residue of a negative residue number $(-A)$ in modulo (2^n) is the 2's complement of A.

$$|-A|_{2^n} = \text{2's complement of } A \tag{1.42}$$

Property 4: The multiplication of a residue number A by 2^p in modulo (2^n) is carried out by p bit left shift and zero filling right p bits, where p is a natural number.

$$|2^p \cdot A|_{2^n} = \text{LS}^0(\text{A, p}) \tag{1.43}$$

where the function LS^0(x, r) is used to denote a shift of the binary number x by r bits to the left and zero filling right r bits.

1.4 Adders and Subtractors:

1.4.1 Basic Adder Unit:

The basic arithmetic operation is the addition of two binary digits, i.e. bits. A combinational circuit that adds two bits is called a half adder. A full adder is one that adds three bits, the third bit produced from a previous addition operation. One way of implementing a full adder is to utilize two half adders in its implementation. The full adder is the basic unit of addition employed in all the adders discussed here:

1.4.1.1 Half Adder (HA):

A half adder is used to add two binary digits, a and b. It gives **S**, the sum of a and b, and the corresponding carry out c_{out}. A half adder is not extremely useful, but it can be used as a building block for larger adding circuits (like Full Adder). A simplest half-adder circuit can be implemented using one XOR gate and one AND gate as shown in Fig. 1.1 (a).

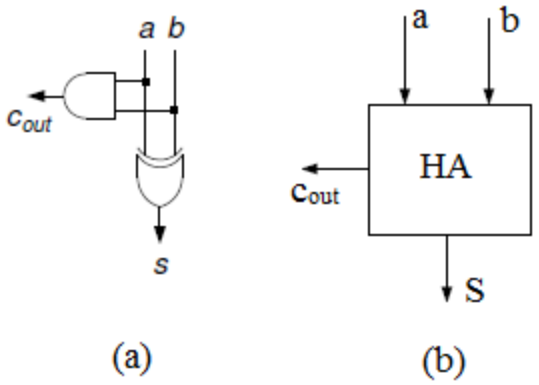


Figure 1.1 (a) Half adder logic (b) Half Adder block diagram [22]

1.4.1.2 Full Adder (FA):

A full adder is a combinational circuit that performs the arithmetic sum of three bits: a, b and an optional carry in, c_{in}, from a previous addition. Similar to half adder, a full adder also produces a sum, S, and a carry out c_{out}. As mentioned previously a full adder maybe designed by two half adders in series as shown below in Fig. 1.2 (a).

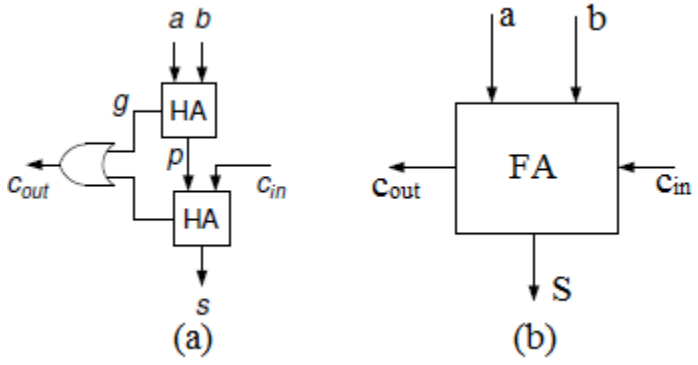


Figure 1.2 (a) Full adder logic (b) Full Adder block diagram [22]

1.4.2 Carry Propagate Adder (CPA):

A CPA adds two n-bit operands A and B and an optional carry-in c_{in} by performing carry propagation. It is constructed by cascading full adder blocks in series. One full adder is responsible for the addition of two binary digits at any stage of the carry propagation. The carryout of one stage is fed directly to the carry-in of the next stage. An n-bit CPA requires n FA's. The delay of a CPA is n times the delay of a FA.

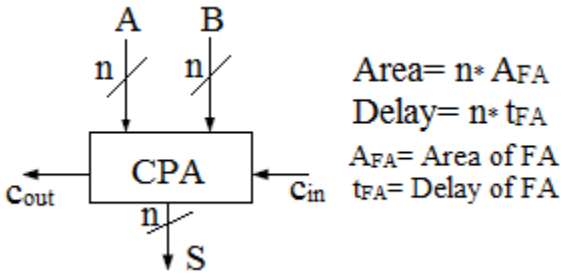


Figure 1.3 Block diagram of CPA [22]

This CPA can be useful in implementing property 1 of equation (1.40) by ignoring carry out, i.e., 2's complement addition of A and B. Therefore this adder acts as a modulo (2^n) adder (if carry out is ignored).

1.4.2.1 CPA as Subtractor:

A CPA of Fig. 1.3 can be used as subtractor by inputting a carry-in (c_{in}) value of one and 1's complement of *B*. This is a 2's complement subtractor.

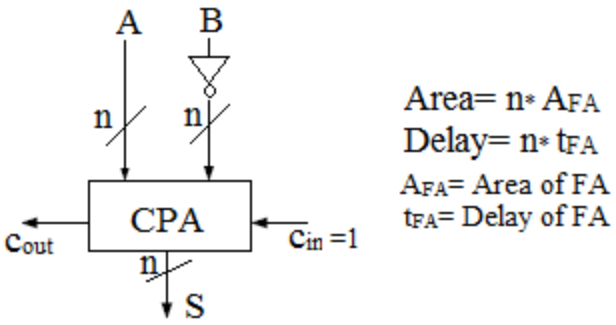


Figure 1.4 Block diagram of CPA as subtractor [22]

1.4.3 Carry Propagate Adder with End Around Carry (CPA with EAC):

A CPA with EAC adds two n-bit operands A and B and end around carry by performing carry propagation. Its construction and operation is similar to CPA, except the carry out of the final stage is fed back to CPA as carry-in. An n-bit CPA with EAC requires n FA's. The delay of a CPA with EAC is twice the delay of regular CPA, i.e., 2n times the delay of a FA for a cost effective version [15].

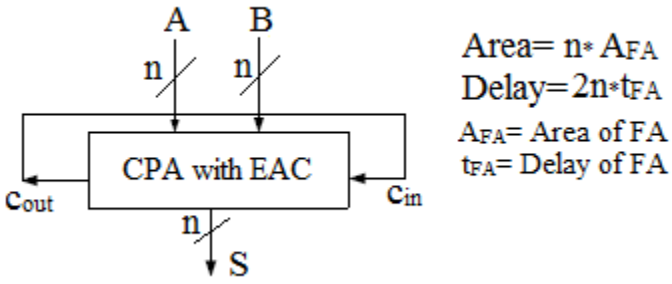


Figure 1.5 Block diagram of CPA with EAC [22]

A CPA with EAC is 1's complement adder and helpful in implementing properties 1 and 2 of equations (1.36) and (1.37). This adder does modulo$(2^n - 1)$ addition of n-bit operands A and B, and hence it is a modulo$(2^n - 1)$ adder.

1.4.4 Carry Save Adder (CSA):

A CSA adds three n-bit input operands (A, B and C) and produces two outputs, i.e., n-bit Sum S and Carry C. The results S and C are summed up with a carry propagate adder or any other adder. Unlike normal adders (e.g., ripple carry – carry propagate adder (RCA) and carry-look ahead adder (CLA)), a CSA contains no carry propagation. Therefore, the CSA has the same propagation delay as only one FA delay (compared to CPA's n FA delay), and the delay is constant for any value of n.

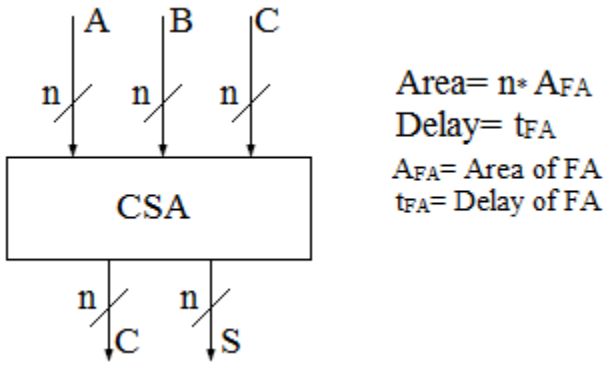


Figure 1.6 Block diagram of CSA [22]

1.4.5 Carry Save Adder with End Around Carry (CSA with EAC):

A CSA with EAC adds three n-bit input operands (A, B and C) and produces two outputs, i.e., n-bit Sum S and Carry C. The results S and C are summed up with a CPA with EAC or CSA with EAC while most significant carry bit C_n is ended around for addition. The area and delay of this adder is same as that of regular CSA. The Fig. 1.7 shows the addition of three 3-bit operands A, B and C using CSA with EAC and the subsequent addition of result using CPA with EAC [17].

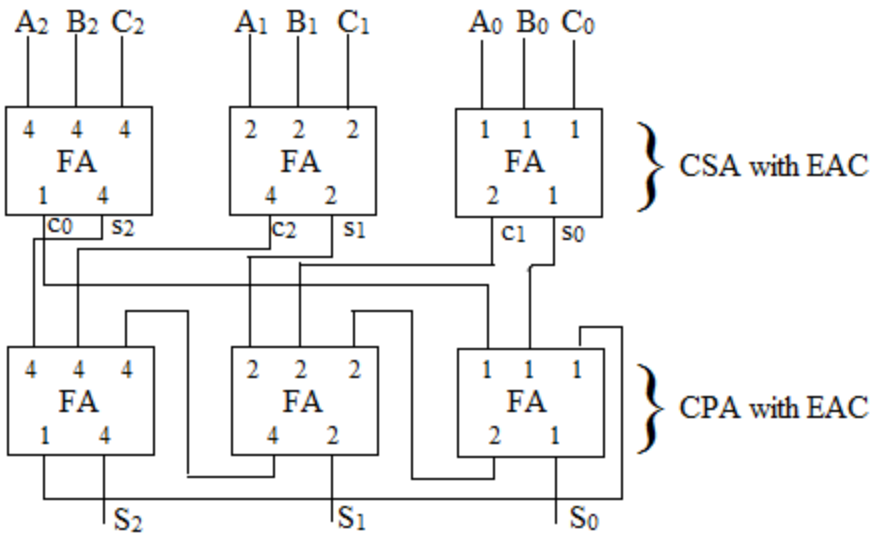


Figure 1.7 Logic Scheme of Adding three 3-bit operands A, B, & C using CSA/CPA with EAC [17]

A CSA with EAC is 1's complement adder of three input operands and helpful in implementing properties 1 and 2 of equations (1.36) and (1.37) for addition of three input operands A, B and C. This adder does modulo$(2^n - 1)$ addition of three n-bit operands (A, B and C), and hence it is a modulo$(2^n - 1)$ adder.

1.4.6 Multi-operand Modulo $(2^n - 1)$ Addition (MOMA):

A (N, $2^n - 1$) MOMA [15], [16] adds N n-bit input operands using n-bit CSA with EAC tree and reduces N input operands to two n-bit operands Sum S and Carry C. The results S and C are summed up with an n-bit CPA with EAC. This MOMA is useful in implementing properties 1 and 2 of equations (1.36) and (1.37) for modulo$(2^n - 1)$ addition of N input operands, therefore it is a modulo $(2^n - 1)$ adder. The tree of adders requires (N-2) CSA's with EAC. The minimum number of levels *l* on a CSA tree that processes N input operands is calculated using a formula defined in [17]. The Table 1.1 gives the minimum number of levels *l* required to build the CSA tree for different values of N.

Table 1.1 The Minimum Number of Levels *l* on a CSA tree that processes N input operands [17]

N	3	4	5-6	7-9	10-13	14-19	20-28	29-42	43-63
l	1	2	3	4	5	6	7	8	9

The area and delay of a (N, $2^n - 1$) MOMA is given below:

Area= $(N-2)Area_{n-bit\ CSA\ with\ EAC\ tree} + Area_{n-bit\ CPA\ with\ EAC} = (N-2) * n\ A_{FA} + n\ A_{FA}$

Delay= $Delay_{n-bit\ CSA\ with\ EAC\ tree} + Delay_{n-bit\ CPA\ with\ EAC} = l * t_{FA} + 2n * t_{FA}$

where $A_{FA}$is the Area of a Full Adder, t_{FA} is the delay of a Full Adder and *l* is the minimum number of levels of the CSA tree.

The Fig. 1.8 shows the addition of seven n-bit operands A, B, C, D, E, F, and G using CSA with EAC tree and the subsequent addition of result using CPA with EAC, i.e., using a (7, $2^n - 1$) MOMA.

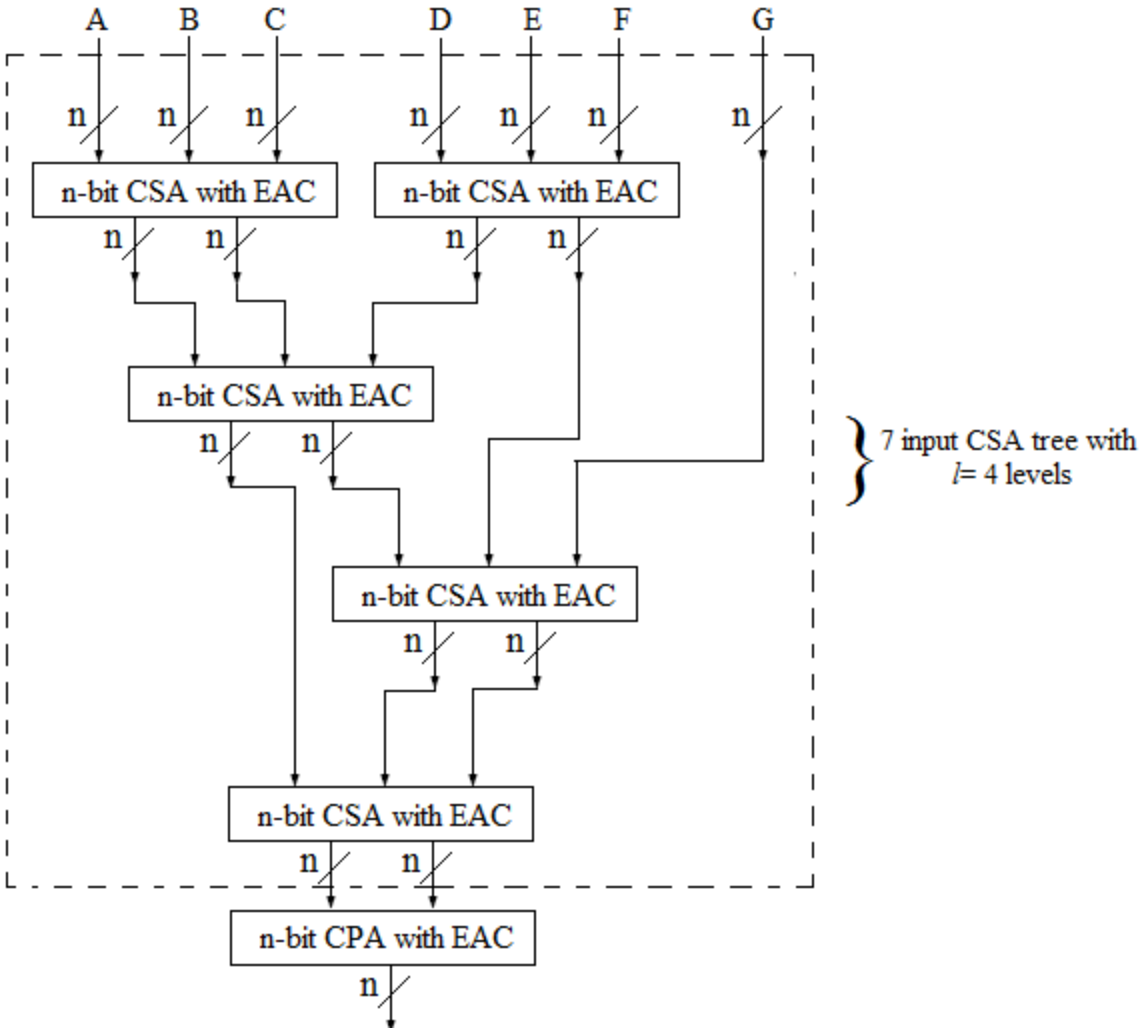


Figure 1.8 Block Diagram of the (7, $2^n - 1$) MOMA using CSA/CPA with EAC [17]

2. DESIGN OF REVERSE CONVERTERS FOR FOUR MODULI SETS

2.1 Four Moduli Sets:

The four moduli sets P_1', P_1 and P_2 shown below have been proposed by Abdallah and Skavantzos in [18] for radix r. In this research, these four moduli sets have been considered and reverse converters are designed for binary domain, i.e. for radix r=2. The importance of these moduli sets is that they contain the moduli of forms 2^a, 2^b- 1, 2^c + 1 (a, b and c are natural numbers) which can be efficiently implemented using usual binary hardware that leads to simple design and offers speed-cost benefits. The reverse converters are designed by applying any one or combination of two or more conversion algorithms discussed in Section 1.2.4. Also, in designing these converters modulo (2^n) and modulo ($2^n - 1$) adders discussed in Section 1.4 are used because these modulo adders lead to simple design of adder based architectures and efficient VLSI implementations. The four moduli sets P_1', P_1 and P_2 are given below:

$$P_1' = \{2^{n-1} - 1, 2^n - 1, 2^n, 2^n + 1\}, \text{where } n = 2k, k = 2, 3, 4, \ldots \quad (2.1)$$

$$P_1 = \{2^{n-1} - 1, 2^{n-1} + 1, 2^n, 2^n + 1\}, \text{where } n = 2k, k = 2, 3, 4, \ldots \quad (2.2)$$

$$P_2 = \{2^{n-1} + 1, 2^n - 1, 2^n, 2^n + 1\}, \text{where } n = 2k + 1, k = 2, 3, 4, \ldots \quad (2.3)$$

2.1.1 Reverse Converter Designs for $P_1' = \{2^{n-1} - 1, 2^n - 1, 2^n, 2^n + 1\}$:

Consider the four moduli set $P_1' = \{2^n, 2^{n-1} - 1, 2^n + 1, 2^n - 1\} = \{m_1, m_2, m_3, m_4\}$, where n is even natural number (n>2) and let the corresponding residues of the integer X be (x_1, x_2, x_3, x_4). The residues have bit-level representations as:

$$x_1 = (x_{1,n-1}x_{1,n-2} \ldots x_{1,1}x_{1,0})_2 \quad (2.4)$$

$$x_2 = (x_{2,n-2}x_{2,n-3} \ldots x_{2,1}x_{2,0})_2 \quad (2.5)$$

$$x_3 = (x_{3,n}x_{3,n-1} \dots x_{3,1}x_{3,0})_2 \tag{2.6}$$

$$x_4 = (x_{4,n-1}x_{4,n-2} \dots x_{4,1}x_{4,0})_2 \tag{2.7}$$

The Sections 2.1.1.1, 2.1.1.2, and 2.1.1.3 describe the design of reverse converters using different conversion algorithms.

2.1.1.1 Reverse Converter Design for P_1' Using New CRT II:

The value of *X* is calculated from New CRT II as follows:

$$X = Z + m_1 m_2 |k_1(Y - Z)|_{m_3 m_4} \tag{2.8}$$

where

$$Z = x_1 + m_1 \mid k_2(x_2 - x_1) \mid_{m_2} \tag{2.9}$$

$$Y = x_3 + m_3 \mid k_3(x_4 - x_3) \mid_{m_4} \tag{2.10}$$

$$k_1 = |(m_1 m_2)^{-1}|_{m_3 m_4},\ k_2 = |m_1^{-1}|_{m_2} \text{ and } k_3 = |m_3^{-1}|_{m_4} \tag{2.11}$$

The following propositions are needed for the derivation of *X*.

Proposition 1: The multiplicative inverse of 2^n modulo $2^{n-1} - 1$ is:

$$|m_1^{-1}|_{m_2} = |(2^n)^{-1}|_{2^{n-1}-1} = 2^{n-2} \tag{2.12}$$

where n is any even number larger than 2.

Proof: The property of equation (1.35) defines if $|a^{-1}|_m = b$ then $|a \cdot b|_m = 1$

Since $|(2^n)^{-1}|_{2^{n-1}-1} = 2^{n-2}$, we have

$$|2^n \cdot 2^{n-2}|_{2^{n-1}-1} = |2^{n-1} \cdot 2^{n-1}|_{2^{n-1}-1} = |1 \cdot 1|_{2^{n-1}-1} = 1$$

Proposition 2: The multiplicative inverse of $2^n + 1$ modulo $2^n - 1$ is:

$$|m_3^{-1}|_{m_4} = |(2^n + 1)^{-1}|_{2^n-1} = 2^{n-1} \tag{2.13}$$

where n is any even number larger than 2.

Proof: Using inverse modulo property of equation (1.35).

Since $|(2^n+1)^{-1}|_{2^n-1} = 2^{n-1}$, we have

$$|(2^n+1)2^{n-1}|_{2^n-1} = |(2)2^{n-1}|_{2^n-1} = |2^n|_{2^n-1} = 1$$

Proposition 3: The multiplicative inverse of $(2^n \cdot (2^{n-1}-1))$ modulo $2^{2n}-1$ is:

$$|(m_1 m_2)^{-1}|_{m_3 m_4} = |(2^n \cdot (2^{n-1}-1))^{-1}|_{2^{2n}-1} = \sum_{l=2}^{n} 2^l + \sum_{m=n+3}^{2n-1} 2^m \qquad (2.14)$$

where n is even(n>2), *l* is even and m is odd. The above expression contains $(n-1)$ terms.

Examples: The following values of multiplicative inverse for different values of n are found using the program given in Appendix A (Section A.2).

The value of $|(2^n \cdot (2^{n-1}-1))^{-1}|_{2^{2n}-1}$ for different values of n is:

For $n = 4$, $|(2^n \cdot (2^{n-1}-1))^{-1}|_{2^{2n}-1} = |112^{-1}|_{255}$=148

$$= (10010100)_2 \; in \; binary$$

$$= 2^2 + 2^4 + 2^7$$

$$= 2^2 + 2^n + 2^{n+3}$$

For $n = 6$, $|(2^n \cdot (2^{n-1}-1))^{-1}|_{2^{2n}-1} = |1984^{-1}|_{4095}$=2644

$$= (101001010100)_2$$

$$= 2^2 + 2^4 + 2^6 + 2^9 + 2^{11}$$

$$= 2^2 + 2^4 + 2^n + 2^{n+3} + 2^{2n-1}$$

For $n = 8$, $|(2^n \cdot (2^{n-1}-1))^{-1}|_{2^{2n}-1} = |32512^{-1}|_{65535}$=43348

$$= (1010100101010100)_2$$

$$= 2^2 + 2^4 + 2^6 + 2^8 + 2^{11} + 2^{13} + 2^{15}$$

$$= 2^2 + 2^4 + 2^6 + 2^n + 2^{n+3} + 2^{n+5} + 2^{2n-1}$$

Thus the above values of $|(2^n \cdot (2^{n-1}-1))^{-1}|_{2^{2n}-1}$ can be generalized as follows,

$$|(2^n \cdot (2^{n-1}-1))^{-1}|_{2^{2n}-1} = \sum_{l=2}^{n} 2^l + \sum_{m=n+3}^{2n-1} 2^m \ , where\ l\ is\ even\ and\ m\ is\ odd$$

First, we simplify the equation (2.9) by substituting the value of equation (2.12) as follows:

$$Z = x_1 + 2^n \mid 2^{n-2}(x_2 - x_1) \mid_{2^{n-1}-1} = x_1 + 2^n M \tag{2.15}$$

where

$$M = |a_1 + a_2 |_{2^{n-1}-1} \tag{2.16}$$

$$a_1 = |2^{n-2}x_2 |_{2^{n-1}-1} = |2^{n-2}(\underbrace{x_{2,n-2}x_{2,n-3} \dots x_{2,1}}_{n-2}\underbrace{x_{2,0}}_{1})|_{2^{n-1}-1}$$

using property 4 of equation (1.39), we have

$$a_1 = \underbrace{x_{2,0}}_{1}\underbrace{x_{2,n-2}x_{2,n-3} \dots x_{2,1}}_{n-2} \tag{2.17}$$

$$a_2 = | - 2^{n-2}x_1 |_{2^{n-1}-1} = | - 2^{n-2}(x_{1,n-1}x_{1,n-2} \dots x_{1,1}x_{1,0})|_{2^{n-1}-1}$$

$$= | - 2^{n-2}\left(x_{1,n-1} \cdot 2^{n-1} + x_{1,n-2}x_{1,n-3} \dots x_{1,1}x_{1,0}\right)|_{2^{n-1}-1}$$

$$= | - 2^{n-2}\left(x_{1,n-1} + x_{1,n-2}x_{1,n-3} \dots x_{1,1}x_{1,0}\right)|_{2^{n-1}-1} = |a_{21} + a_{22} |_{2^{n-1}-1}$$

here, $$a_{21} = | - 2^{n-2}(\underbrace{x_{1,n-2}x_{1,n-3} \dots x_{1,2}x_{1,1}}_{n-2}\underbrace{x_{1,0}}_{1})|_{2^{n-1}-1}$$

using property 3, 4 of equations (1.38) and (1.39), we have

$$a_{21} = \underbrace{\overline{x_{1,0}}}_{1}\underbrace{\overline{x_{1,n-2}x_{1,n-3} \dots x_{1,2}x_{1,1}}}_{n-2} \tag{2.18}$$

and

$$a_{22} = | - 2^{n-2}(\underbrace{00 \dots 00}_{n-2}\underbrace{x_{1,n-1}}_{1})|_{2^{n-1}-1}$$

using property 3, 4 of equations (1.38) and (1.39), we have

$$a_{22} = \underbrace{\overline{x_{1,n-1}}}_{1}\underbrace{11 \dots 11}_{n-2} \tag{2.19}$$

Therefore, the equation (2.16) can be rewritten as

$$M = |a_1 + a_{21} + a_{22}|_{2^{n-1}-1} \tag{2.20}$$

Next, equation (2.10) can be rewritten by substituting value of equation (2.13) as:

$$Y = x_3 + (2^n + 1) \mid 2^{n-1}(x_4 - x_3) \mid_{2^n-1} = x_3 + (2^n + 1)N \tag{2.21}$$

where

$$N = |a_3 + a_4 \,|_{2^n-1} \tag{2.22}$$

$$a_3 = |2^{n-1}x_4 \,|_{2^n-1} = |2^{n-1}(\underbrace{x_{4,n-1}x_{4,n-2} \dots x_{4,1}}_{n-1}\underbrace{x_{4,0}}_{1})|_{2^n-1}$$

$$a_3 = \underbrace{x_{4,0}}_{1}\underbrace{x_{4,n-1}x_{4,n-2} \dots x_{4,1}}_{n-1} \tag{2.23}$$

$$a_4 = |-2^{n-1}x_3 \,|_{2^n-1}$$

Since, x_3 is a number that is smaller than$2^n + 1$, we can consider two cases for x_3. First, when x_3 is smaller than 2^n, and the second, when x_3 is equal to 2^n. If $x_{3,n} = 0$, we have

$$a_{41} = | - 2^{n-1}(\underbrace{x_{3,n-1} \dots x_{3,2}x_{3,1}}_{n-1}\underbrace{x_{3,0}}_{1})|_{2^n-1}$$

$$= \underbrace{\overline{x_{3,0}}}_{1}\underbrace{\overline{x_{3,n-1} \dots x_{3,2}x_{3,1}}}_{n-1} \tag{2.24}$$

Else if $x_{3,n} = 1$, the following binary number can be obtained as

$$a_{42} = | - 2^{n-1} \times 2^n(\underbrace{0 \dots 00}_{n-1}\underbrace{x_{3,n}}_{1})|_{2^n-1} = 0\,\underbrace{1 \dots 11}_{n-1} \tag{2.25}$$

Therefore, a_4 is calculated as

$$a_4 = \begin{cases} a_{41} & if \;\; x_{3,n} = 0 \\ a_{42} & if \;\; x_{3,n} = 1 \end{cases} \tag{2.26}$$

Finally, equation (2.8) can be simplified as

$$X = Z + 2^n(2^{n-1} - 1)| - k_1(Z - Y)|_{2^{2n}-1} = Z + 2^n(2^{n-1} - 1)P \tag{2.27}$$

where

$$P = |-k_1 T|_{2^{2n}-1} \text{ and } T = |(Z-Y)|_{2^{2n}-1} \tag{2.28}$$

The value of T is simplified as:

$$\begin{aligned} T &= |x_1 + 2^n M - x_3 - (2^n+1)N|_{2^{2n}-1} \\ &= |a_5 + a_6 + a_7 + a_8|_{2^{2n}-1} \end{aligned} \tag{2.29}$$

where

$$a_5 = |(\underbrace{0 \dots 00}_{n} \underbrace{x_{1,n-1}x_{1,n-2} \dots x_{1,1}x_{1,0}}_{n})|_{2^{2n}-1}$$

$$= \underbrace{0 \dots 00}_{n} \underbrace{x_{1,n-1}x_{1,n-2} \dots x_{1,1}x_{1,0}}_{n} \tag{2.30}$$

$$a_6 = |2^n M|_{2^{2n}-1} = |2^n(\underbrace{0 \dots 00}_{n+1} \underbrace{M_{n-2}M_{n-3} \dots M_1 M_0}_{n-1})|_{2^{2n}-1}$$

$$= \underbrace{0}_{1} \underbrace{M_{n-2}M_{n-3} \dots M_1 M_0}_{n-1} \underbrace{0 \dots 00}_{n} \tag{2.31}$$

$$a_7 = |-(\underbrace{0 \dots 00}_{n-1} \underbrace{x_{3,n}x_{3,n-1} \dots x_{3,1}x_{3,0}}_{n+1})|_{2^{2n}-1}$$

$$= \underbrace{1 \dots 11}_{n-1} \underbrace{\overline{x_{3,n}x_{3,n-1} \dots x_{3,1}x_{3,0}}}_{n+1} \tag{2.32}$$

$$a_8 = |-(2^n+1)N|_{2^{2n}-1} = |-(2^n+1)(\underbrace{N_{n-1}N_{n-2} \dots N_1 N_0}_{n})|_{2^{2n}-1}$$

$$= |-(\underbrace{N_{n-1}N_{n-2} \dots N_1 N_0}_{n} \underbrace{N_{n-1}N_{n-2} \dots N_1 N_0}_{n})|_{2^{2n}-1}$$

$$= \underbrace{\overline{N_{n-1}N_{n-2} \dots N_1 N_0}}_{n} \underbrace{\overline{N_{n-1}N_{n-2} \dots N_1 N_0}}_{n} \tag{2.33}$$

The value of a_8 in equation (2.33) can be combined with a_5, a_6 to give a_5' and a_6' as follows:

$$a_5' = \underbrace{\overline{N_{n-1}N_{n-2} \dots N_1 N_0}}_{n} \underbrace{x_{1,n-1}x_{1,n-2} \dots x_{1,1}x_{1,0}}_{n} \tag{2.34}$$

$$a_6' = \underbrace{0}_{1} \underbrace{M_{n-2}M_{n-3} \dots M_1 M_0}_{n-1}) \underbrace{\overline{N_{n-1}N_{n-2} \dots N_1 N_0}}_{n} \tag{2.35}$$

Therefore, the equation (2.29) can be rewritten as:

$$T = |a_5' + a_6' + a_7|_{2^{2n}-1} \tag{2.36}$$

The value of *P* in equation (2.28) can be simplified by substituting value of equation (2.14) as:

$$P = |-k_1 T|_{2^{2n}-1} = |-\left(\sum_{l=2}^{n} 2^l + \sum_{m=n+3}^{2n-1} 2^m \right) T|_{2^{2n}-1}$$

$$=|-(2^2 + 2^4 + \cdots + 2^n)T - (2^{n+3} + 2^{n+5} \ldots . + 2^{2n-1})T|_{2^{2n}-1}$$

$$=|CLS(\bar{T}, 2) + CLS(\bar{T}, 4) + \cdots + CLS(\bar{T}, n) + CLS(\bar{T}, n+3) +$$

$$CLS(\bar{T}, n+5) \ldots + CLS(\bar{T}, 2n-1)|_{2^{2n}-1} \tag{2.37}$$

The value of *X* in equation (2.27) can be simplified by substituting equation (2.15) as:

$$X = Z + 2^n(2^{n-1} - 1)P = x_1 + 2^n M + 2^n(2^{n-1} - 1)P$$

$$= x_1 + 2^n(M + (2^{n-1} - 1)P)$$

$$= x_1 + 2^n Q \tag{2.38}$$

where

$$Q = M + (2^{n-1} - 1)P = M + 2^{n-1}P - P = K - P \tag{2.39}$$

$$K = M + 2^{n-1}P = \underbrace{P_{2\,n-1}P_{2n-2} \ldots P_1 P_0}_{2n} \underbrace{M_{n-2}M_{n-3} \ldots M_1 M_0}_{n-1} \tag{2.40}$$

Also, since x_1 is an n-bit number, *X* in (2.38) can be obtained as

$$X = x_1 + 2^n Q = \underbrace{Q_{3n-2}Q_{3n-3} \ldots Q_1 Q_0}_{3n-1} \underbrace{x_{1,n-1}x_{1,n-2} \ldots x_{1,1}x_{1,0}}_{n} \tag{2.41}$$

Example: Consider the moduli set $\{2^n, 2^{n-1} - 1, 2^n + 1, 2^n - 1\}$ where n=4. The weighted number *X* can be calculated from its RNS representation (7, 6, 10, 8) as follow:

For n=4 the moduli set is {16, 7, 17, 15} and also residues have binary representation as below

$$x_1 = 7 = (0111)_2$$

$$x_2 = 6 = (110)_2$$

$$x_3 = 10 = (01010)_2$$

$$x_4 = 8 = (1000)_2$$

By letting the values of residues and n=4 in equations (2.17), (2.18), (2.19), (2.16), (2.23), (2.24), (2.26), and (2.22) we have

$$a_1 = (011)_2 = 3$$

$$a_{21} = (000)_2 = 0$$

$$a_{22} = (111)_2 = 7$$

$$M = |3 + 0 + 7|_7 = |10|_7 = 3 = (011)_2$$

$$a_3 = (0100)_2 = 4$$

$$a_{41} = (1010)_2 = 10$$

$$a_4 = a_{41}$$

$$N = |4 + 10|_{15} = |14|_{15} = 14 = (1110)_2$$

Then, the required values should be substituted in (2.33), (2.34), (2.31), and (2.35)

$$a'_5 = (00010111)_2 = 23$$

$$a'_6 = (00110001)_2 = 49$$

$$a_7 = (11110101)_2 = 245$$

$$T = |23 + 49 + 245|_{255} = 62 = (00111110)_2$$

$$\bar{T} = (11000001)_2$$

$$CLS(\bar{T}, 2) = (00000111)_2 = 7$$

$$CLS(\bar{T}, 4) = (00011100)_2 = 28$$

$$CLS(\bar{T}, 7) = (11100000)_2 = 224$$

Finally, by letting the values of *M*, *T*, and x_1 in (2.37), (2.40), (2.39) and (2.41), *X* can be computed as follows:

$$P = |CLS(\bar{T}, 2) + CLS(\bar{T}, 4) + CLS(\bar{T}, 7)|_{255} = |7 + 28 + 224|_{255} = 4 = (00000100)_2$$

$$K = \underbrace{00000100}_{8}\,\underbrace{011}_{3} = 35$$

$$Q = K - P = 35 - 4 = 31 = (00000011111)_2$$

$$X = \underbrace{00000011111}_{11}\,\underbrace{0111}_{4} = 503$$

To verify the result, we have

$$x_1 = |503|_{16} = 7$$

$$x_2 = |503|_7 = 6$$

$$x_3 = |503|_{17} = 10$$

$$x_4 = |503|_{15} = 8$$

Therefore, the weighted number 503 in the RNS based on the 4-moduli set {16, 7, 17, 15} has representation as (7, 6, 10, 8).

Hardware Implementation: The reverse converter hardware architecture for the four moduli set $\{2^n, 2^{n-1} - 1, 2^n + 1, 2^n - 1\}$ with corresponding residues (x_1, x_2, x_3, x_4) of the integer X is shown in Fig. 2.1. Implementation is based on equations (2.20), (2.22), (2.36), (2.37), (2.39) and (2.41). Firstly, the operand preparation unit 1 (OPU 1) prepares the required operands of (2.17), (2.18), (2.19), (2.23) and (2.26) and these operand preparations rely on simply manipulating the routing of the bits of residues. Also, we need 2n NOT gates for performing inversions needed in (2.18), (2.19) and (2.24). In addition, an n-bit 2×1 multiplexer (MUX) is used for obtaining (2.26). Implementation of (2.20) requires a 4-operand modulo $(2^{n-1} - 1)$ adder, and it can be implemented by one $(n - 1)$ bit CSA1 with EAC and one $(n - 1)$ CPA2 with EAC. Also, since (2.19) has $(n - 2)$ bits of 1's, $(n - 2)$ FA's of CSA1 are reduced to $(n - 2)$ pairs of XNOR/OR gates. Implementation of (2.22) requires one n-bit CPA1

with EAC modulo $(2^n - 1)$ adder. The OPU 2 requires (2n+1) NOT gates to prepare operands of (2.34), (2.35) and (2.32). Implementation of (2.36) requires 3-operand modulo $(2^{2n} - 1)$ adder that relies on one 2n bit CSA2 with EAC followed by 2n bit CPA3 with EAC. Also, since (2.35) has 1 bit of 0 and (2.32) has $(n - 1)$ bits of 1's, n FA's in CSA2 are reduced to the pairs of 1 XOR/AND and (n-1) XNOR/OR gates. The OPU 3 does bit orientation on (2.36) for (2.37) and requires 2n NOT gates to invert bits in (2.36). Realization of (2.37) requires $(n - 1, 2^{2n}$-1) MOMA, and it can be implemented by one 2n bit CSA3 with EAC tree followed by a 2n bit CPA4 with EAC. The CSA3 tree has (n-3) 2n-bit CSA's with EAC arranged in *l*- levels. Finally, the implementation of (2.39) requires a 3n-1 bit regular binary subtractor. This subtractor can be realized by 2n NOT gates (to invert (2.37) in OPU 3), 2n FA's and (n-1) pairs of XNOR/OR gates. It should be noted that realization of (2.40) and (2.41) rely on simple concatenation without the use of any computational hardware. Area and Delay specification for each part of the converter are shown in Table 2.1.

2.1.1.2 Reverse Converter Design for P_1' Using CRT and MRC:

The reverse converter design for P_1' using CRT and MRC has been discussed in [19]. A detailed derivation of this algorithm with hardware and delay specifications is presented in this section. The set P_1' is decomposed into two subsets $A_1 = \{2^n, 2^{n-1} - 1\}, A_2 = \{2^n + 1, 2^n - 1\}$. Two interim integers $X^{(1)}$ and $X^{(2)}$ are calculated from the residues x_1, x_2 of A_1 and x_3, x_4 of A_2 respectively. The conversion algorithms MRC and CRT are used to calculate $X^{(1)}$ and $X^{(2)}$ respectively. Next, the MRC algorithm is applied to calculate the final integer *X* from the residues $(X^{(1)}, X^{(2)})$ corresponding to the moduli set $A_3 = \{2^n(2^{n-1} - 1), (2^{2n} - 1)\}$. The

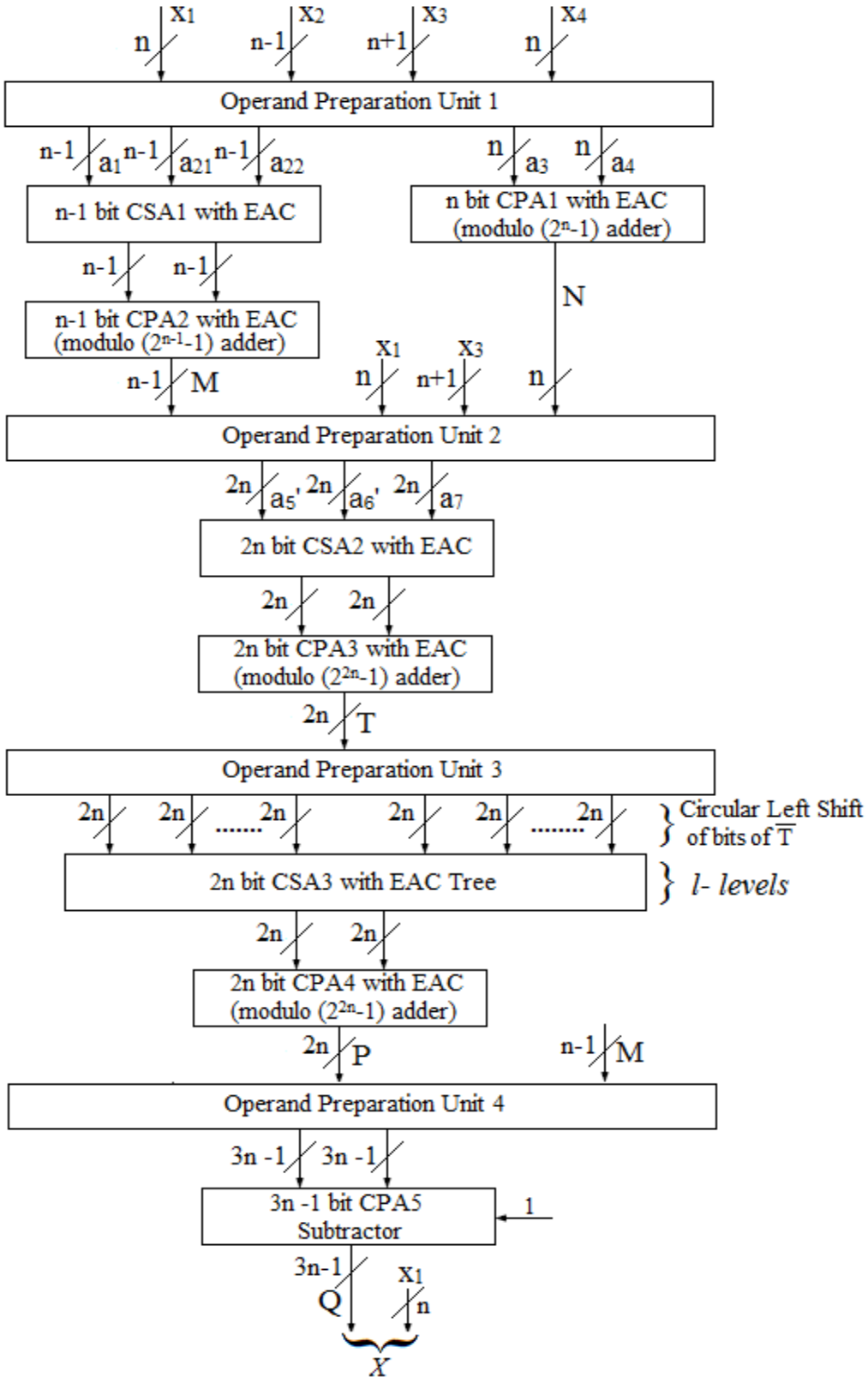


Figure 2.1 Reverse Converter for the moduli set P_1' using New CRT II

Table 2.1

Hardware and Delay Specification of Reverse Converter for the moduli set P_1' using New CRT-II

Parts	**FA**	**NOT**	**XOR/AND pairs**	**XNOR/OR pairs**	**MUX 2×1**	**Delay**
OPU 1		2n			1(n) -bit	$t_{NOT} + t_{MUX}$
CSA1	1			n-2		t_{FA}
CPA1	n					$2n\ t_{FA}$
CPA2	n-1					$(2n-2)t_{FA}$
OPU 2		2n+1				t_{NOT}
CSA2	n		1	n-1		t_{FA}
CPA3	2n					$4n\ t_{FA}$
OPU 3		2n				t_{NOT}
CSA3 Tree	$2n^2$ -6n					$l \cdot t_{FA}$
CPA4	2n					$4n\ t_{FA}$
OPU 4		2n				t_{NOT}
CPA5	2n			n-1		$(3n-1)t_{FA}$
Total Area		$(2n^2+3n)A_{FA}$+ (8n+1)A_{NOT}+ A_{XOR}+ A_{AND}+ (3n-4)A_{XNOR}+ (3n-4) A_{OR} + $A_{MUX(n)}$				
Total Delay		$(13n+l)t_{FA}$ + $4t_{NOT}$ + t_{MUX}				

Here l is the minimum number of levels of CSA tree required to process n-1 input operands.

following proposition and the propositions 1, 2, 3 of equations (2.12), (2.13), (2.14) are needed for the derivation of *X*.

Proposition 1: The multiplicative inverse of $2^n - 1$ modulo $2^n + 1$ is:

$$|m_4^{-1}|_{m_3} = |(2^n - 1)^{-1}|_{2^n+1} = 2^{n-1} \tag{2.42}$$

where n is any even number larger than 2

Proof: Using inverse modulo property of equation (1.35).

Since $|(2^n - 1)^{-1}|_{2^n+1} = 2^{n-1}$, we have

$$|(2^n - 1)2^{n-1}|_{2^n+1} = |(-2)2^{n-1}|_{2^n+1} = |-2^n|_{2^n+1} = |2^n + 1 - 2^n|_{2^n+1} = 1$$

Calculation of $X^{(1)}$:

The value of $X^{(1)}$ is calculated from MRC as follows:

$$X^{(1)} = x_1 + m_1 \cdot | \, |m_1^{-1}|_{m_2} \cdot (x_2 - x_1) \, |_{m_2} \tag{2.43}$$

Substituting the value (2.12), m_1 and m_2 in (2.43) we have

$$X^{(1)} = x_1 + 2^n \cdot | \, 2^{n-2} \cdot (x_2 - x_1) \, |_{2^{n-1}-1}$$

$$= x_1 + 2^n M = \underbrace{M_{n-2}M_{n-3} \dots M_1 M_0}_{n-1} \underbrace{x_{1,n-1}x_{1,n-2} \dots x_{1,1}x_{1,0}}_{n} \tag{2.44}$$

where

$$M = | \, a_1 + a_{21} + a_{22} \, |_{2^{n-1}-1} \tag{2.45}$$

$$a_1 = \underbrace{x_{2,0}}_{1} \underbrace{x_{2,n-2}x_{2,n-3} \dots x_{2,1}}_{n-2} \tag{2.46}$$

$$a_{21} = \underbrace{\overline{x_{1,0}}}_{1} \underbrace{\overline{x_{1,n-2} \dots x_{1,1}}}_{n-2} \tag{2.47}$$

$$a_{22} = \underbrace{\overline{x_{1,n-1}}}_{1} \underbrace{1 \dots 11}_{n-2} \tag{2.48}$$

Calculation of $X^{(2)}$:

The value of $X^{(2)}$ is calculated from CRT as follows:

$$X^{(2)} = |\, x_3 m_4 |m_4^{-1}|_{m_3} + x_4 m_3 |m_3^{-1}|_{m_4}|_{m_3 m_4} \tag{2.49}$$

Substituting the values (2.13) and (2.42) in (2.49) we have

$$X^{(2)} = |\, x_3(2^{2n-1} - 2^{n-1}) + x_4(2^{2n-1} + 2^{n-1})|_{2^{2n}-1}$$

$$= |\, a_3 + a_4 + a_5|_{2^{2n}-1} \tag{2.50}$$

where

$$a_3 = \underbrace{x_{3,0}}_{1}\, \underbrace{0 \ldots 00}_{n-1}\, \underbrace{x_{3,n} x_{3,n-1} \ldots x_{3,1}}_{n} \tag{2.51}$$

$$a_4 = \underbrace{\overline{x_{3,n} x_{3,n-1} \ldots x_{3,1} x_{3,0}}}_{n+1}\, \underbrace{1 \ldots 11}_{n-1} \tag{2.52}$$

$$a_5 = \underbrace{x_{4,0}}_{1}\, \underbrace{x_{4,n-1} x_{4,n-2} \ldots x_{4,1} x_{4,0}}_{n}\, \underbrace{x_{4,n-1} x_{4,n-2} \ldots x_{4,1}}_{n-1} \tag{2.53}$$

Calculation of X:

The value of X is calculated from MRC as follows:

$$X = X^{(1)} + 2^n(2^{n-1} - 1)||(2^n \cdot 2^{n-1} - 1)^{-1}|_{2^{2n}-1}(X^{(2)} - X^{(1)})|_{2^{2n}-1}$$

$$= X^{(1)} + 2^n(2^{n-1} - 1)P \tag{2.54}$$

where

$$P = ||(2^n \cdot 2^{n-1} - 1)^{-1}|_{2^{2n}-1} N|_{2^{2n}-1} \tag{2.55}$$

$$N = |\, a_6 + a_7|_{2^{2n}-1} \tag{2.56}$$

$$a_6 = \underbrace{X_{2n-1}^{(2)} X_{2n-2}^{(2)} \ldots X_1^{(2)} X_0^{(2)}}_{2n} \tag{2.57}$$

$$a_7 = \underbrace{1}_{1}\, \underbrace{\overline{X_{2n-2}^{(1)} X_{2n-3}^{(1)} \ldots X_1^{(1)} X_0^{(1)}}}_{2n-1} \tag{2.58}$$

Substituting the value of (2.14) in (2.55) we have

$$P = |CLS(N,2) + CLS(N,4) + \cdots + CLS(N,n) +$$

$$CLS(N,n+3) + CLS(N,n+5) \ldots + CLS(N,2n-1)|_{2^{2n}-1} \tag{2.59}$$

Now, *X* can be rewritten as

$$X = x_1 + 2^n M + 2^n(2^{n-1} - 1)P$$
$$= x_1 + 2^n(M + (2^{n-1} - 1)P)$$
$$= x_1 + 2^n Q \quad (2.60)$$

where

$$Q = M + 2^{n-1}P - P = K - P \quad (2.61)$$

$$K = M + 2^{n-1}P = \underbrace{P_{2\,n-1}P_{2n-2} \dots P_1 P_0}_{2n}\,\underbrace{M_{n-2}M_{n-3} \dots M_1 M_0}_{n-1} \quad (2.62)$$

Also, since x_1 is an n-bit number, *X* in (2.60) can be obtained as

$$X = x_1 + 2^n Q = \underbrace{Q_{3n-2}Q_{3n-3} \dots Q_1 Q_0}_{3n-1}\,\underbrace{x_{1,n-1}x_{1,n-2} \dots x_{1,1}x_{1,0}}_{n} \quad (2.63)$$

Example: Consider the moduli set $\{2^n, 2^{n-1} - 1, 2^n + 1, 2^n - 1\}$ where n=4. The weighted number *X* can be calculated from its RNS representation (15, 0, 15, 2) as follow

For n=4 the moduli set is {16, 7, 17, 15} and also residues have binary representation as below

$x_1 = 15 = (1111)_2$

$x_2 = 0 = (000)_2$

$x_3 = 15 = (01111)_2$

$x_4 = 2 = (0010)_2$

According to (2.46), (2.47), (2.48), (2.45), (2.44), (2.51), (2.52), (2.53), (2.50), (2.57), (2.58), and (2.59) we have

$a_1 = (000)_2 = 0$

$a_{21} = (000)_2 = 0$

$$a_{22} = (011)_2 = 3$$

$$M = |3|_7 = (011)_2 = 3$$

$$X^{(1)} = (0111111)_2 = 63$$

$$a_3 = (10000111)_2 = 135$$

$$a_4 = (10000111)_2 = 135$$

$$a_5 = (00010001)_2 = 17$$

$$X^{(2)} = |287|_{255} = 32 = (00100000)_2$$

$$a_6 = (00100000)_2 = 32$$

$$a_7 = (11000000)_2 = 192$$

$$N = |224|_{255} = 224 = (11100000)_2$$

$$P = |33152|_{255} = 2 = (00000010)_2$$

Substituting the values of *M* and *P* in (2.62) and (2.61), *X* can be calculated as below

$$K = (00000010011)_2 = 19$$

$$Q = K - P = 19 - 2 = 17 = (00000010001)_2$$

$$X = (000000100011111)_2 = 287$$

We can see that $|287|_{16} = 15$, $|287|_7 = 0$, $|287|_{17} = 15$, $|287|_{15} = 2$, and therefore the calculated *X* is indeed the weighted value of the residue representation (15, 0, 15, 2) with respect to the moduli set {16, 7, 17, 15}.

Hardware Implementation: The reverse converter hardware architecture for the four moduli set $\{2^n, 2^{n-1} - 1, 2^n + 1, 2^n - 1\}$ with corresponding residues (x_1, x_2, x_3, x_4) of the integer *X* is shown in Fig. 2.2. Area and Delay specification for each part of the converter are shown in Table 2.2.

Table 2.2

Area and Delay Specification of Reverse Converter for the moduli set P_1' using CRT and MRC

Parts	**FA**	**NOT**	**XOR/AND pairs**	**XNOR/OR pairs**	**Delay**
OPU 1		2n+1			t_{NOT}
CSA1	1			n-2	t_{FA}
CPA1	n-1				$(2n-2)t_{FA}$
CSA2	2		n-1	n-1	t_{FA}
CPA2	2n				$4n\ t_{FA}$
OPU 2		2n-1			t_{NOT}
CPA3	2n-1			1	$4n\ t_{FA}$
OPU 3	-				-
CSA3 Tree	$2n^2$ -6n				$l \cdot t_{FA}$
CPA4	2n				$4n\ t_{FA}$
OPU 4		2n			t_{NOT}
CPA5	2n			n-1	$(3n-1)t_{FA}$
Total Area	$(2n^2+3n+1)A_{FA}$+ $6nA_{NOT}$+ (n-1)A_{XOR}+ (n-1)A_{AND}+ (3n-3)A_{XNOR}+ (3n-3) A_{OR}				
Total Delay	$(15n+l)t_{FA}$ + $3t_{NOT}$				

Here *l* is the minimum number of levels of CSA tree required to process n-1 input operands.

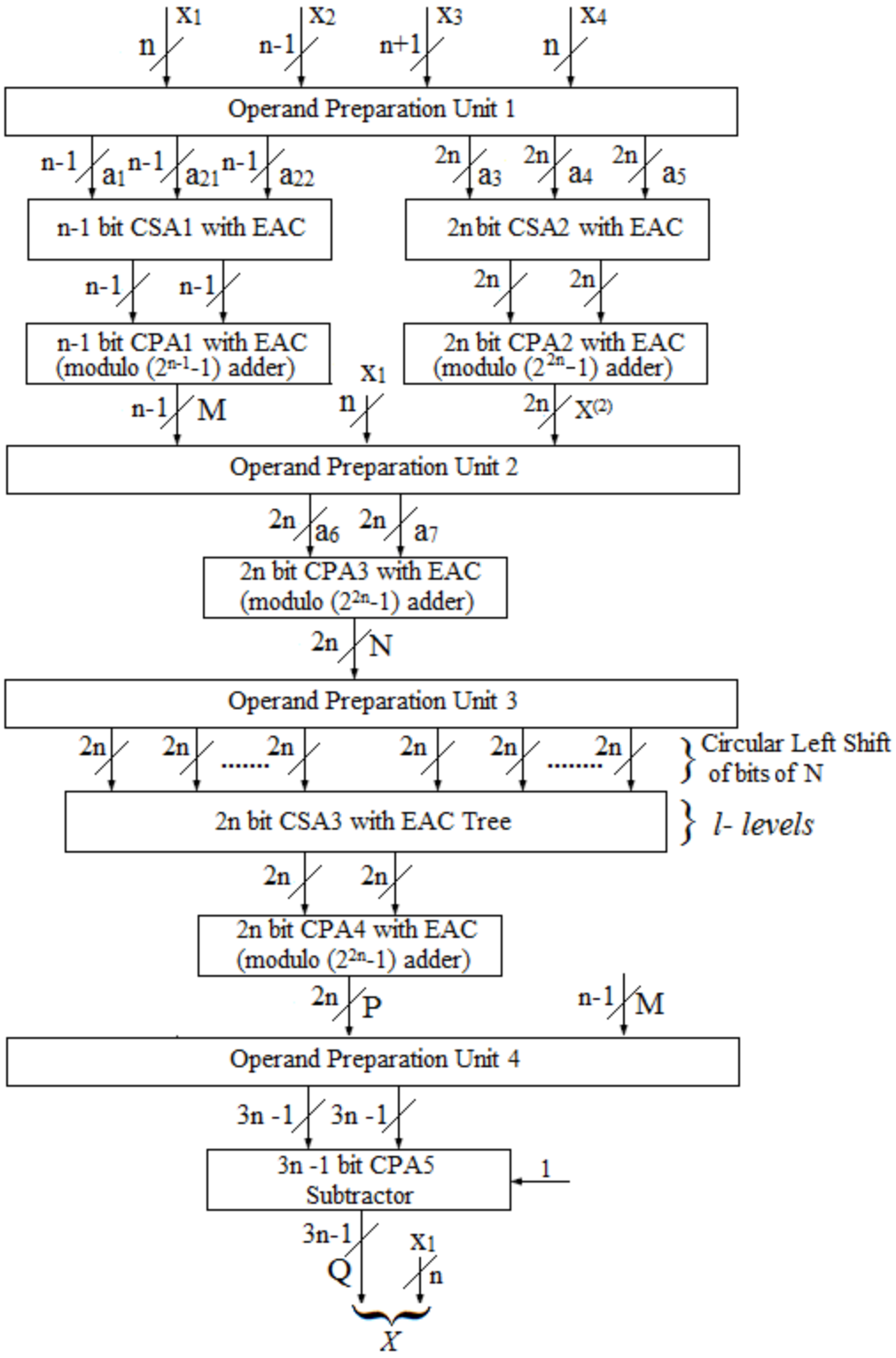


Figure 2.2 Reverse Converter for the moduli set P_1' using CRT and MRC

2.1.1.3 Reverse Converter Design for P_1' Using New CRT I and MRC:

The design of the reverse converter for the four moduli set P_1' using the conversion algorithms New CRT I and MRC has been proposed in [19]. The Area and Delay Specification for this converter is shown in Table 2.3.

Table 2.3

Area and Delay of Reverse Converter for the moduli set P_1' using New CRT I and MRC [19]

Total Area	$0.5*(n^2+17n-6)A_{FA}+(5n+1)A_{NOT}+6A_{XOR}+6A_{AND}+(2n-8)A_{XNOR}+(2n-8)A_{OR}+2A_{MUX(1)}+A_{HA}$
Total Delay	$(11n+l-1)t_{FA}+2t_{NOT}+t_{MUX}$

Here l is the minimum number of levels of CSA tree required to process (n/2) input operands.

2.1.2 Reverse Converter Designs for $P_1 = \{2^{n-1}-1, 2^{n-1}+1, 2^n, 2^n+1\}$:

Consider the four moduli set $P_1 = \{2^n+1, 2^n, 2^{n-1}+1, 2^{n-1}-1\} = \{m_1, m_2, m_3, m_4\}$, where n is even natural number (n>2) and let the corresponding residues of the integer X be (x_1, x_2, x_3, x_4). The residues have bit-level representations as:

$$x_1 = (x_{1,n}x_{1,n-1}\dots x_{1,1}x_{1,0})_2$$

$$x_2 = (x_{2,n-1}x_{2,n-2}\dots x_{2,1}x_{2,0})_2$$

$$x_3 = (x_{3,n-1}x_{3,n-2}\dots x_{3,1}x_{3,0})_2$$

$$x_4 = (x_{4,n-2}x_{4,n-3}\dots x_{4,1}x_{4,0})_2$$

The Sections 2.1.2.1 and 2.1.2.2 describe the design of reverse converters using different conversion algorithms.

2.1.2.1 Reverse Converter Design for P_1 Using New CRT II:

The value of X is calculated from New CRT II as follows:

$$X = Z + m_1 m_2 |k_1 (Y - Z)|_{m_3 m_4} \tag{2.64}$$

where

$$Z = x_1 + m_1 \mid k_2 (x_2 - x_1) \mid_{m_2} \tag{2.65}$$

$$Y = x_3 + m_3 \mid k_3 (x_4 - x_3) \mid_{m_4} \tag{2.66}$$

$$k_1 = |(m_1 m_2)^{-1}|_{m_3 m_4}, k_2 = |m_1^{-1}|_{m_2} \text{ and } k_3 = |m_3^{-1}|_{m_4} \tag{2.67}$$

The following propositions are needed for the derivation of *X*.

Proposition 1: The multiplicative inverse of $2^n + 1$ modulo 2^n is:

$$|m_1^{-1}|_{m_2} = |(2^n + 1)^{-1}|_{2^n} = 1 \tag{2.68}$$

where n is any even number larger than 2.

Proof: The property of equation (1.35) defines if $|a^{-1}|_m = b$ then $| a \cdot b |_m = 1$

Since $= |(2^n + 1)^{-1}|_{2^n} = 1$, we have

$$|2^n + 1|_{2^n} = 1$$

Proposition 2: The multiplicative inverse of $2^{n-1} + 1$ modulo $2^{n-1} - 1$ is:

$$|m_3^{-1}|_{m_4} = |(2^{n-1} + 1)^{-1}|_{2^{n-1}-1} = 2^{n-2} \tag{2.69}$$

where n is any even number larger than 2.

Proof: Using inverse modulo property of equation (1.35).

Since $|(2^{n-1} + 1)^{-1}|_{2^{n-1}-1} = 2^{n-2}$, we have

$$|(2^{n-1} + 1)2^{n-2}|_{2^{n-1}-1} = |(2)2^{n-2}|_{2^{n-1}-1} = |2^{n-1}|_{2^{n-1}-1} = 1$$

Proposition 3: The multiplicative inverse of $(2^n \cdot 2^n + 1)$ modulo $2^{2n-2} - 1$ is:

$$|(m_1 m_2)^{-1}|_{m_3 m_4} = |(2^n \cdot (2^n + 1))^{-1}|_{2^{2n-2}-1} = \sum_{l=0}^{\frac{n-2}{2}} 2^l + \sum_{m=n-1}^{2n-3} 2^m \tag{2.70}$$

where n is even(n>2), *l* is even and m is odd. The above expression contains $(n - 1)$ terms.

Examples: The following values of multiplicative inverse for different values of n are found using the program given in Appendix A (Section A.2).

The value of $|(2^n \cdot 2^n + 1)^{-1}|_{2^{2n-2}-1}$ for different values of n is:

For $n = 4$, $|(2^n \cdot 2^n + 1)^{-1}|_{2^{2n-2}-1} = |272^{-1}|_{63}$=41

$= (101001)_2$ *in binary*

$= 2^0 + 2^3 + 2^5$

$= 2^0 + 2^{n-1} + 2^{2n-3}$

For $n = 6$, $|(2^n \cdot 2^n + 1)^{-1}|_{2^{2n-2}-1} = |4160^{-1}|_{1023}$=677

$= (1010100101)_2$

$= 2^0 + 2^2 + 2^5 + 2^7 + 2^9$

$= 2^0 + 2^{(n-2)/2} + 2^{n-1} + 2^{n+1} + 2^{2n-3}$

For $n = 8$, $|(2^n \cdot 2^n + 1)^{-1}|_{2^{2n-2}-1} = |65792^{-1}|_{16383}$=10901

$= (10101010010101)_2$

$= 2^0 + 2^2 + 2^4 + 2^7 + 2^9 + 2^{11} + 2^{13}$

$= 2^0 + 2^2 + 2^{(n-2)/2} + 2^{n-1} + 2^{n+1} + 2^{n+3} + 2^{2n-3}$

Thus the above values of $|(2^n \cdot 2^{n-1} - 1)^{-1}|_{2^{2n}-1}$ can be generalized as follows,

$$|(2^n \cdot (2^n + 1))^{-1}|_{2^{2n-2}-1} = \sum_{l=0}^{\frac{n-2}{2}} 2^l + \sum_{m=n-1}^{2n-3} 2^m \ , where\ l\ is\ even\ and\ m\ is\ odd$$

First, we simply the equation (2.65) by substituting value of equation (2.68) as follows:

$$Z = x_1 + (2^n + 1) \mid 1(x_2 - x_1) \mid_{2^n} = x_1 + (2^n + 1)M \qquad (2.71)$$

where

$$M = \mid (x_2 - x_1) \mid_{2^n} = |a_1 + a_2 |_{2^n} \qquad (2.72)$$

$$a_1 = |x_2|_{2^n} = \underbrace{x_{2,n-1}x_{2,n-2}\dots x_{2,1}x_{2,0}}_{n} \tag{2.73}$$

$$a_2 = |-x_1|_{2^n} = |-(2^n \underbrace{x_{1,n}}_{1} + \underbrace{x_{1,n-1}\dots x_{1,1}x_{1,0}}_{n})|_{2^n}$$

$$= |0 + \underbrace{\overline{x_{2,n-2}\dots x_{2,1}x_{2,0}}}_{n} + 1|_{2^n}$$

$$= \underbrace{\overline{x_{1,n-1}\dots x_{1,1}x_{1,0}}}_{n} \text{ (+ 1 as Carry-in to CPA)} \tag{2.74}$$

Next, equation (2.16) can be rewritten by substituting value of equation (2.69) as:

$$Y = x_3 + (2^{n-1}+1) \mid 2^{n-2}(x_4 - x_3)\mid_{2^{n-1}-1} = x_3 + (2^{n-1}+1)N \tag{2.75}$$

where

$$N = \mid 2^{n-2}(x_4 - x_3)\mid_{2^{n-1}-1} = |a_3 + a_4|_{2^{n-1}-1} \tag{2.76}$$

$$a_3 = |2^{n-2}x_4|_{2^{n-1}-1} = |2^{n-2}(\underbrace{x_{4,n-2}x_{4,n-3}\dots x_{4,1}}_{n-2}\underbrace{x_{4,0}}_{1})|_{2^{n-1}-1}$$

$$a_3 = \underbrace{x_{4,0}}_{1}\underbrace{x_{4,n-2}x_{4,n-3}\dots x_{4,1}}_{n-2} \tag{2.77}$$

$$a_4 = |-2^{n-2}x_3|_{2^{n-1}-1}$$

Since, x_3 is a number that is smaller than$2^{n-1}+1$, we can consider two cases for x_3. First, when x_3 is smaller than 2^{n-1}, and the second, when x_3 is equal to 2^{n-1}. If $x_{3,n-1} = 0$, we have

$$a_{41} = |-2^{n-2}(\underbrace{x_{3,n-2}\dots x_{3,2}x_{3,1}}_{n-2}\underbrace{x_{3,0}}_{1})|_{2^{n-1}-1}$$

$$= \underbrace{\overline{x_{3,0}}}_{1}\underbrace{\overline{x_{3,n-2}\dots x_{3,2}x_{3,1}}}_{n-2} \tag{2.78}$$

Else if $x_{3,n} = 1$, the following binary number can be obtained as

$$a_{42} = |-2^{n-1}\times 2^{n-1}(\underbrace{0\dots 00}_{n-2}\underbrace{x_{3,n-1}}_{1})|_{2^{n-1}-1} = 0\underbrace{1\dots 11}_{n-2}$$

Therefore, a_4 is calculated as

$$a_4 = \begin{cases} a_{41} & if\ \ x_{3,n-1} = 0 \\ a_{42} & if\ \ x_{3,n-1} = 1 \end{cases} \tag{2.79}$$

Finally, equation (2.64) can be simplified as

$$X = Z + 2^n(2^n + 1)|k_1(Y - Z)|_{2^{2n-2}-1} = Z + 2^n(2^n + 1)P \tag{2.80}$$

where

$$P = |k_1 T|_{2^{2n-2}-1} \text{ and } T = |(Y - Z)|_{2^{2n-2}-1} \tag{2.81}$$

The value of T is simplified as:

$$\begin{aligned} T &= |x_3 + (2^{n-1} + 1)N - x_1 - (2^n + 1)M|_{2^{2n-2}-1} \\ &= |a_5 + a_6 + a_7 + a_8 + a_9|_{2^{2n-2}-1} \end{aligned} \tag{2.82}$$

where

$$\begin{aligned} a_5 &= |(\underbrace{0 \dots 00}_{n-2}\ \underbrace{x_{3,n-1}x_{3,n-2} \dots x_{3,1}x_{3,0}}_{n})|_{2^{2n-2}-1} \\ &= \underbrace{0 \dots 00}_{n-2}\ \underbrace{x_{3,n-1}x_{3,n-2} \dots x_{3,1}x_{3,0}}_{n} \end{aligned} \tag{2.83}$$

$$\begin{aligned} a_6 = |(2^{n-1} + 1)N|_{2^{2n-2}-1} &= |(\underbrace{N_{n-2}N_{n-3} \dots N_1N_0}_{n-1}\ \underbrace{N_{n-2}N_{n-3} \dots N_1N_0}_{n-1})|_{2^{2n-2}-1} \\ &= \underbrace{N_{n-2}N_{n-3} \dots N_1N_0}_{n-1}\ \underbrace{N_{n-2}N_{n-3} \dots N_1N_0}_{n-1} \end{aligned} \tag{2.84}$$

$$\begin{aligned} a_7 &= |-(\underbrace{0 \dots 00}_{n-3}\ \underbrace{x_{1,n}x_{1,n-1} \dots x_{1,1}x_{1,0}}_{n+1})|_{2^{2n-2}-1} \\ &= \underbrace{1 \dots 11}_{n-3}\ \underbrace{\overline{x_{1,n}x_{1,n-1} \dots x_{1,1}x_{1,0}}}_{n+1} \end{aligned} \tag{2.85}$$

$$|a_8 + a_9|_{2^{2n-2}-1} = |-(2^n + 1)M|_{2^{2n-2}-1} = |-(2^n + 1)(\underbrace{M_{n-1}M_{n-2} \dots M_1M_0}_{n})|_{2^{2n-2}-1}$$

$$= |-(\underbrace{0 \dots 00}_{n-2}\ \underbrace{M_{n-1}M_{n-2}}_{2} + \underbrace{M_{n-3}M_{n-4} \dots M_1M_0}_{n-2}\ \underbrace{M_{n-1}M_{n-2} \dots M_1M_0}_{n})|_{2^{2n-2}-1}$$

$$\begin{aligned} a_8 &= \underbrace{1 \dots 11}_{2n-4}\ \underbrace{\overline{M_{n-1}M_{n-2}}}_{2} \end{aligned} \tag{2.86}$$

$$a_9 = \overline{\underbrace{M_{n-3}M_{n-4}\dots M_1M_0}_{n-2}\ \underbrace{M_{n-1}M_{n-2}\dots M_1M_0}_{n}} \tag{2.87}$$

The value of *P* in equation (2.81) can be simplified by substituting value of equation (2.70) as:

$$P = |k_1T|_{2^{2n-2}-1} = |(\sum_{l=0}^{\frac{n-2}{2}} 2^l + \sum_{m=n-1}^{2n-3} 2^m)T|_{2^{2n-2}-1}$$

$$=|\left(2^0 + 2^2 \dots + 2^{(n-2)/2}\right)T + (2^{n-1} + 2^{n+1} \dots + 2^{2n-3})T|_{2^{2n-2}-1}$$

$$=|CLS(T,0) + CLS(T,2) + \cdots + CLS(T,(n-2)/2) + CLS(T,n-1) +$$

$$CLS(T,n+1) \dots + CLS(T,2n-3)|_{2^{2n-2}-1} \tag{2.88}$$

The value of *X* in equation (2.80) can be simplified by substituting *Z* as:

$$X = Z + 2^n(2^n+1)P = x_1 + (2^n+1)M + 2^n(2^n+1)P$$

$$= x_1 + (2^n+1)(M + 2^nP)$$

$$= x_1 + (2^n+1)Q$$

$$= a_{10} + a_{11} + a_{12} \tag{2.89}$$

where

$$a_{10} = \underbrace{0\dots00}_{3n-3}\ \underbrace{x_{1,n}}_{1}\ \underbrace{0\dots00}_{n} \tag{2.90}$$

$$a_{11} = \underbrace{Q_{3n-3}Q_{3n-4}\dots Q_1Q_0}_{3n-2}\ \underbrace{x_{1,n-1}x_{1,n-2}\dots x_{1,1}x_{1,0}}_{n} \tag{2.91}$$

$$a_{12} = \underbrace{0\dots00}_{n}\ \underbrace{Q_{3n-3}Q_{3n-4}\dots Q_1Q_0}_{3n-2} \tag{2.92}$$

Example: Consider the moduli set $\{2^n+1, 2^n, 2^{n-1}+1, 2^{n-1}-1\}$ where n=4. The weighted number *X* can be calculated from its RNS representation (12, 11, 7, 4) as follow

For n=4 the moduli set is {17, 16, 9, 7} and also residues have binary representation as below

$$x_1 = 12 = (01100)_2$$

$$x_2 = 11 = (1011)_2$$

$$x_3 = 7 = (0111)_2$$

$$x_4 = 4 = (100)_2$$

According to (2.73), (2.74), (2.72), (277), (2.78), (2.76), (2.83), (2.84), (2.85), (2.86), (2.87), (2.82), and (2.88) we have

$$a_1 = (1011)_2 = 11$$

$$a_2 = (0011)_2\ (+1\ as\ carry\ in\ to\ CPA) = 4$$

$$M = |15|_{16} = (1111)_2 = 15$$

$$a_3 = (010)_2 = 2$$

$$a_4 = a_{41} = (000)_2 = 0$$

$$N = |2|_7 = (010)_2 = 2$$

$$a_5 = (000111)_2 = 7$$

$$a_6 = (010010)_2 = 18$$

$$a_7 = (110011)_2 = 51$$

$$a_8 = (111100)_2 = 60$$

$$a_9 = (000000)_2 = 0$$

$$T = |136|_{63} = 10 = (001010)_2$$

$$P = |410|_{63} = 32 = (100000)_2$$

Substituting the values of *M* and *P* in *Q* and simplifying (2.90), (2.91) and (2.92), *X* can be calculated from (2.89) as below

$$a_{10} = (00000000000000)_2 = 0$$

$$a_{11} = (10000011111100)_2 = 8444$$

$$a_{12} = (00001000001111)_2 = 527$$

$$X = 0 + 8444 + 527 = 8971$$

We can see that $|8971|_{17} = 12,\ |8971|_{16} = 11,\ |8971|_9 = 7,\ |8971|_7 = 4$, and therefore the calculated *X* is indeed the weighted value of the residue representation (12, 11, 7, 4) with respect to the moduli set {17, 16, 9, 7}.

Hardware Implementation: The reverse converter hardware architecture for the four moduli set $\{2^n + 1, 2^n, 2^{n-1} + 1, 2^{n-1} - 1\}$ with corresponding residues (x_1, x_2, x_3, x_4) of the integer *X* is shown in Fig. 2.3. Area and Delay specification for each part of the converter are shown in Table 2.4.

2.1.2.2 Reverse Converter Design for P_1 Using CRT and MRC:

The set P_1 here is decomposed into two subsets $A_1 = \{2^n + 1, 2^n\}, A_2 = \{2^{n-1} + 1, 2^{n-1} - 1\}$. Two interim integers $X^{(1)}$ and $X^{(2)}$ are calculated from the residues x_1, x_2 of A_1 and x_3, x_4 of A_2 respectively. The conversion algorithms MRC and CRT are used to calculate $X^{(1)}$ and $X^{(2)}$ respectively. Next, the MRC algorithm is applied to calculate the final integer *X* from the residues $(X^{(1)},\ X^{(2)})$ corresponding to the moduli set $A_3 = \{2^n(2^n + 1),\ (2^{2n-2} - 1)\}$. The following proposition and the propositions 1, 2, 3 of equations (2.68), (2.69), (2.70) are needed for the derivation of *X*.

Proposition 1: The multiplicative inverse of $2^{n-1} - 1$ modulo $2^{n-1} + 1$ is:

$$|m_4^{-1}|_{m_3} = |(2^{n-1} - 1)^{-1}|_{2^{n-1}+1} = 2^{n-2} \qquad (2.93)$$

where n is any even number larger than 2

Proof: Using inverse modulo property of equation (1.35).

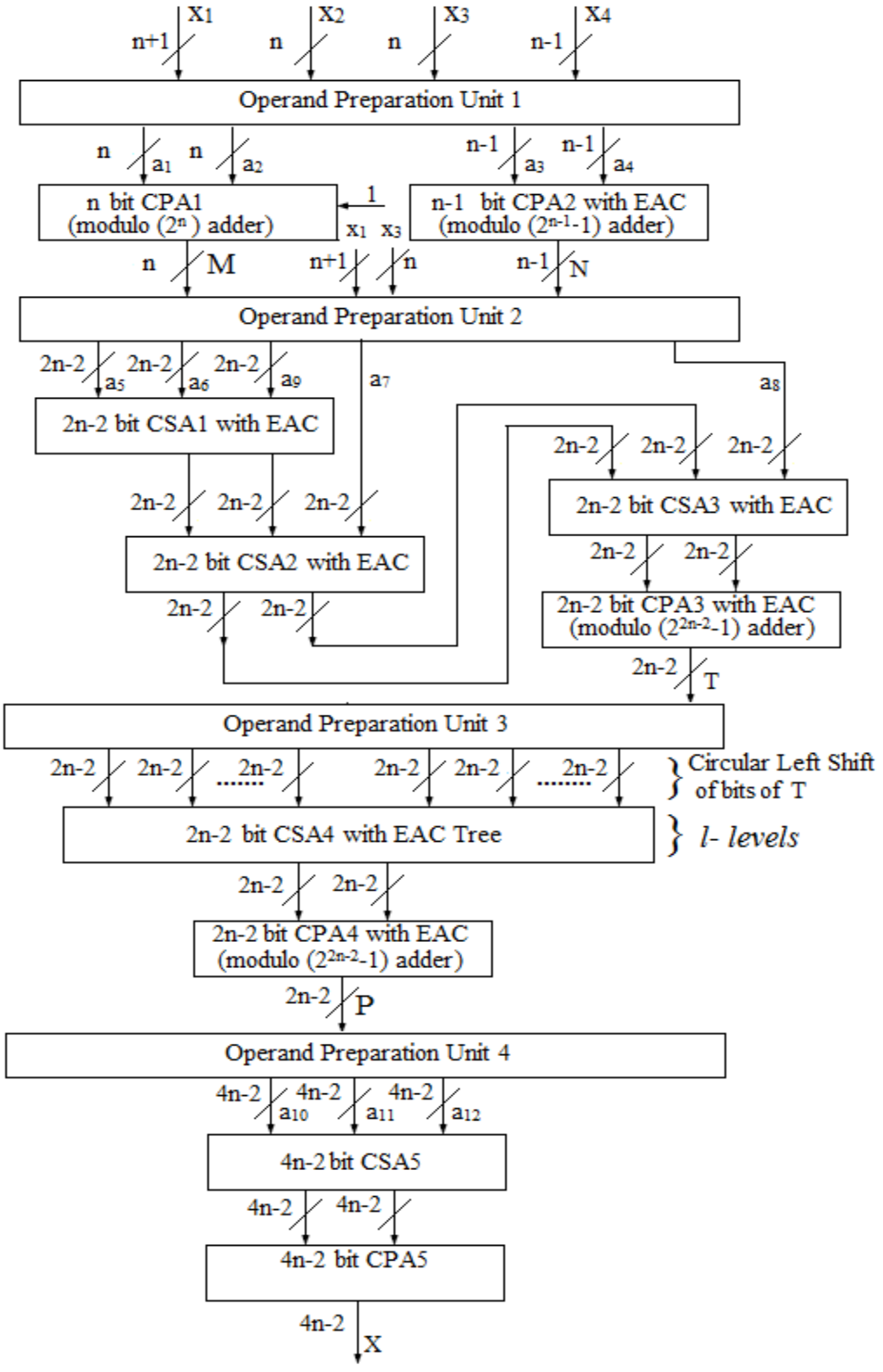


Figure 2.3 Reverse Converter for the moduli set P_1 using New CRT II

Table 2.4

Area and Delay Specification of Reverse Converter for the moduli set P_1 using New CRT II

Parts	**FA**	**NOT**	**XOR/AND pairs**	**XNOR/OR pairs**	**MUX 2×1**	**Delay**
OPU 1		2n-1			1(n-1) -bit	$t_{NOT} + t_{MUX}$
CPA1	n					$n\ t_{FA}$
CPA2	n-1					$(2n-2)t_{FA}$
OPU2		2n+1				t_{NOT}
CSA1	n		n-2			t_{FA}
CSA2	n+1			n-3		t_{FA}
CSA3	2			2n-4		t_{FA}
CPA3	2n-2					$(4n-4)t_{FA}$
OPU3	-					-
CSA4 Tree	$2n^2$-8n+6					$l \cdot t_{FA}$
CPA4	2n-2					$(4n-4)\ t_{FA}$
OPU4	-					-
CSA5	1		4n-3			t_{FA}
CPA5	4n-2					$(4n-2)\ t_{FA}$
Total Area		$(2n^2+4n+3)A_{FA}$+ (4n)A_{NOT}+ (5n-5)A_{XOR}+ (5n-5)A_{AND}+ (3n-7)A_{XNOR}+ (3n-7)A_{OR} + $A_{MUX(n-1)}$				
Total Delay		(14n-8+l)t_{FA} + 2t_{NOT} + t_{MUX}				

Here l is the minimum number of levels of CSA tree required to process n-1 input operands.

Since $|(2^{n-1}-1)^{-1}|_{2^{n-1}+1} = 2^{n-2}$, we have

$$|(2^{n-1}-1)2^{n-2}|_{2^{n-1}+1} = |-2\cdot 2^{n-2}|_{2^{n-1}+1} = |-2^{n-1}|_{2^{n-1}+1}$$
$$= |2^{n-1}+1-2^{n-1}|_{2^{n-1}+1} = 1$$

Calculation of $X^{(1)}$:

The value of $X^{(1)}$ is calculated from MRC as follows:

$$X^{(1)} = x_1 + m_1 \cdot |\,|m_1^{-1}|_{m_2}\cdot(x_2-x_1)\,|_{m_2} \tag{2.94}$$

Substituting the value (2.68), m_1 and m_2 in (2.94) we have

$$X^{(1)} = x_1 + (2^n+1)\,|\,1(x_2-x_1)\,|_{2^n}$$
$$= x_1 + (2^n+1)M \tag{2.95}$$

where

$$M = |\,(x_2-x_1)\,|_{2^n} = |a_1+a_2\,|_{2^n} \tag{2.96}$$

$$a_1 = |x_2\,|_{2^n} = \underbrace{x_{2,n-1}x_{2,n-2}\ldots x_{2,1}x_{2,0}}_{n} \tag{2.97}$$

$$a_2 = |-x_1\,|_{2^n} = |-(2^n\underbrace{x_{1,n}}_{1} + \underbrace{x_{1,n-1}\ldots x_{1,1}x_{1,0}}_{n})|_{2^n}$$
$$= |0+\overline{\underbrace{x_{2,n-2}\ldots x_{2,1}x_{2,0}}_{n}}+1|_{2^n}$$
$$= \underbrace{\overline{x_{1,n-1}\ldots x_{1,1}x_{1,0}}}_{n} \text{ (+ 1 as Carry-in to CPA)} \tag{2.98}$$

Calculation of $X^{(2)}$:

The value of $X^{(2)}$ is calculated from CRT as follows:

$$X^{(2)} = |\,x_3m_4|m_4^{-1}|_{m_3} + x_4m_3|m_3^{-1}|_{m_4}|_{m_3m_4} \tag{2.99}$$

Substituting the values (2.69) and (2.93) in (2.99) we have

$$X^{(2)} = |\,x_3(2^{2n-3}-2^{n-2}) + x_4(2^{2n-3}+2^{n-2})|_{2^{2n-2}-1}$$
$$= |\,a_3+a_4+a_5|_{2^{2n-2}-1} \tag{2.100}$$

where

$$a_3 = \underbrace{x_{3,0}}_{1}\,\underbrace{0\ldots00}_{n-2}\,\underbrace{x_{3,n-1}x_{3,n-2}\ldots x_{3,1}}_{n-1} \tag{2.101}$$

$$a_4 = \underbrace{\overline{x_{3,n-1}x_{3,n-2}\ldots x_{3,1}x_{3,0}}}_{n}\,\underbrace{1\ldots11}_{n-2} \tag{2.102}$$

$$a_5 = \underbrace{x_{4,0}}_{1}\,\underbrace{x_{4,n-2}x_{4,n-3}\ldots x_{4,1}x_{4,0}}_{n-1}\,\underbrace{x_{4,n-2}x_{4,n-3}\ldots x_{4,1}}_{n-2} \tag{2.103}$$

Calculation of X:

The value of X is calculated from MRC as follows:

$$X = X^{(1)} + 2^n(2^n+1)||(2^n\cdot(2^n+1))^{-1}|_{2^{2n-2}-1}(X^{(2)} - X^{(1)})|_{2^{2n-2}-1}$$

$$= X^{(1)} + 2^n(2^n+1)P \tag{2.104}$$

where

$$P = ||(2^n\cdot(2^n+1))^{-1}|_{2^{2n-2}-1}N|_{2^{2n-2}-1} \tag{2.105}$$

$$N = |\left(X^{(2)} - X^{(1)}\right)|_{2^{2n-2}-1} = |\left(X^{(2)} - (x_1 + \ (2^n+1)M)\right)|_{2^{2n-2}-1}$$

$$= |\ a_6 + a_7 + a_8 + a_9|_{2^{2n-2}-1} \tag{2.106}$$

$$a_6 = \underbrace{X_{2n-3}^{(2)}X_{2n-4}^{(2)}\ldots X_1^{(2)}X_0^{(2)}}_{2n-2} \tag{2.107}$$

$$a_7 = \underbrace{1\ldots11}_{n-3}\,\underbrace{\overline{x_{1,n}x_{1,n-1}\ldots x_{1,1}x_{1,0}}}_{n+1} \tag{2.108}$$

$$a_8 = \underbrace{1\ldots11}_{2n-4}\,\underbrace{\overline{M_{n-1}M_{n-2}}}_{2} \tag{2.109}$$

$$a_9 = \underbrace{\overline{M_{n-3}\ldots M_1M_0}}_{n-2}\,\underbrace{\overline{M_{n-1}\ldots M_1M_0}}_{n} \tag{2.110}$$

Substituting the value of (2.70) in (2.105) we have

$$P = |CLS(N,0) + CLS(N,2) + \cdots + CLS\left(N,\frac{n-2}{2}\right) +$$

$$CLS(N,n-1) + CLS(N,n+1)\ldots + CLS(N,2n-3)|_{2^{2n-2}-1} \tag{2.111}$$

Now, *X* in (2.104) can be rewritten as

$$\begin{aligned} X &= x_1 + (2^n + 1)M + 2^n(2^n + 1)P \\ &= x_1 + (2^n + 1)(M + 2^n P) \\ &= x_1 + (2^n + 1)Q \\ &= a_{10} + a_{11} + a_{12} \end{aligned} \tag{2.112}$$

where

$$a_{10} = \underbrace{0 \dots 00}_{3n-3}\ \underbrace{x_{1,n}}_{1}\ \underbrace{0 \dots 00}_{n} \tag{2.113}$$

$$a_{11} = \underbrace{Q_{3n-3}Q_{3n-4} \dots Q_1Q_0}_{3n-2}\ \underbrace{x_{1,n-1}x_{1,n-2} \dots x_{1,1}x_{1,0}}_{n} \tag{2.114}$$

$$a_{12} = \underbrace{0 \dots 00}_{n}\ \underbrace{Q_{3n-3}Q_{3n-4} \dots Q_1Q_0}_{3n-2} \tag{2.115}$$

Example: Consider the moduli set $\{2^n + 1, 2^n, 2^{n-1} + 1, 2^{n-1} - 1\}$ where n=4. The weighted number *X* can be calculated from its RNS representation (13, 8, 6, 4) as follows:

For n=4 the moduli set is {17, 16, 9, 7} and also residues have binary representation as below

$$x_1 = 13 = (01101)_2$$

$$x_2 = 8 = (1000)_2$$

$$x_3 = 6 = (0110)_2$$

$$x_4 = 4 = (100)_2$$

According to (2.97), (2.98), (2.96), (2.101), (2.102), (2.103), (2.100), (2.107), (2.108), (2.109), (2.110), (2.106) and (2.111) we have

$$a_1 = (1000)_2 = 8$$

$$a_2 = (0010)_2\ (+1\ as\ carry\ in) = 3$$

$$M = |11|_{16} = (1011)_2 = 11$$

$$a_3 = (000011)_2 = 3$$

$$a_4 = (100111)_2 = 39$$

$$a_5 = (010010)_2 = 18$$

$$X^{(2)} = |60|_{63} = 60 = (111100)_2$$

$$a_6 = (111100)_2 = 60$$

$$a_7 = (110010)_2 = 50$$

$$a_8 = (11101)_2 = 61$$

$$a_9 = (000100)_2 = 4$$

$$N = |175|_{63} = 49 = (110001)_2$$

$$P = |2009|_{63} = 56 = (111000)_2$$

Substituting the values of *M* and *P* in *Q* and simplifying (2.113), (2.114), (2.115), *X* can be calculated from (2.112) as below

$$a_{10} = (00000000000000)_2 = 0$$

$$a_{11} = (11100010111101)_2 = 14525$$

$$a_{12} = (00001110001011)_2 = 907$$

$$X = 0 + 14525 + 907 = 15432$$

We can see that $|15432|_{17} = 13,\ |15432|_{16} = 8,\ |15432|_9 = 6,\ |15432|_7 = 4$, and therefore the calculated *X* is indeed the weighted value of the residue representation (13, 8, 6, 4) with respect to the moduli set {17, 16, 9, 7}.

Hardware Implementation: The reverse converter hardware architecture for the four moduli set $\{2^n + 1, 2^n, 2^{n-1} + 1, 2^{n-1} - 1\}$ with corresponding residues (x_1, x_2, x_3, x_4) of the integer *X* is shown in Fig. 2.4. Area and Delay specification for each part of the converter are shown in Table 2.5.

Table 2.5

Area and Delay Specification of Reverse Converter for the moduli set P_1 using CRT and MRC

Parts	**FA**	**NOT**	**XOR/AND pairs**	**XNOR/OR pairs**	**Delay**
OPU 1		2n			t_{NOT}
CPA1	n				$n\,t_{FA}$
CSA1	2		n-2	n-2	t_{FA}
CPA2	2n-2				$(4n-4)t_{FA}$
OPU2		2n+1			t_{NOT}
CSA2	n+1			n-3	t_{FA}
CSA3	2			2n-4	t_{FA}
CPA3	2n-2				$(4n-4)t_{FA}$
OPU3	-				-
CSA4 Tree	$2n^2$-8n+6				$l \cdot t_{FA}$
CPA4	2n-2				$(4n-4)\ t_{FA}$
OPU4	-				-
CSA5	1		4n-3		t_{FA}
CPA5	4n-2				$(4n-2)\ t_{FA}$
Total Area		$(2n^2+4n+4)A_{FA}+(4n)A_{NOT}+(5n-5)A_{XOR}+(5n-5)A_{AND}+(3n-7)A_{XNOR}+(3n-7)A_{OR}$			
Total Delay		$(16n-10+l)t_{FA}+2t_{NOT}$			

Here l is the minimum number of levels of CSA tree required to process n-1 input operands.

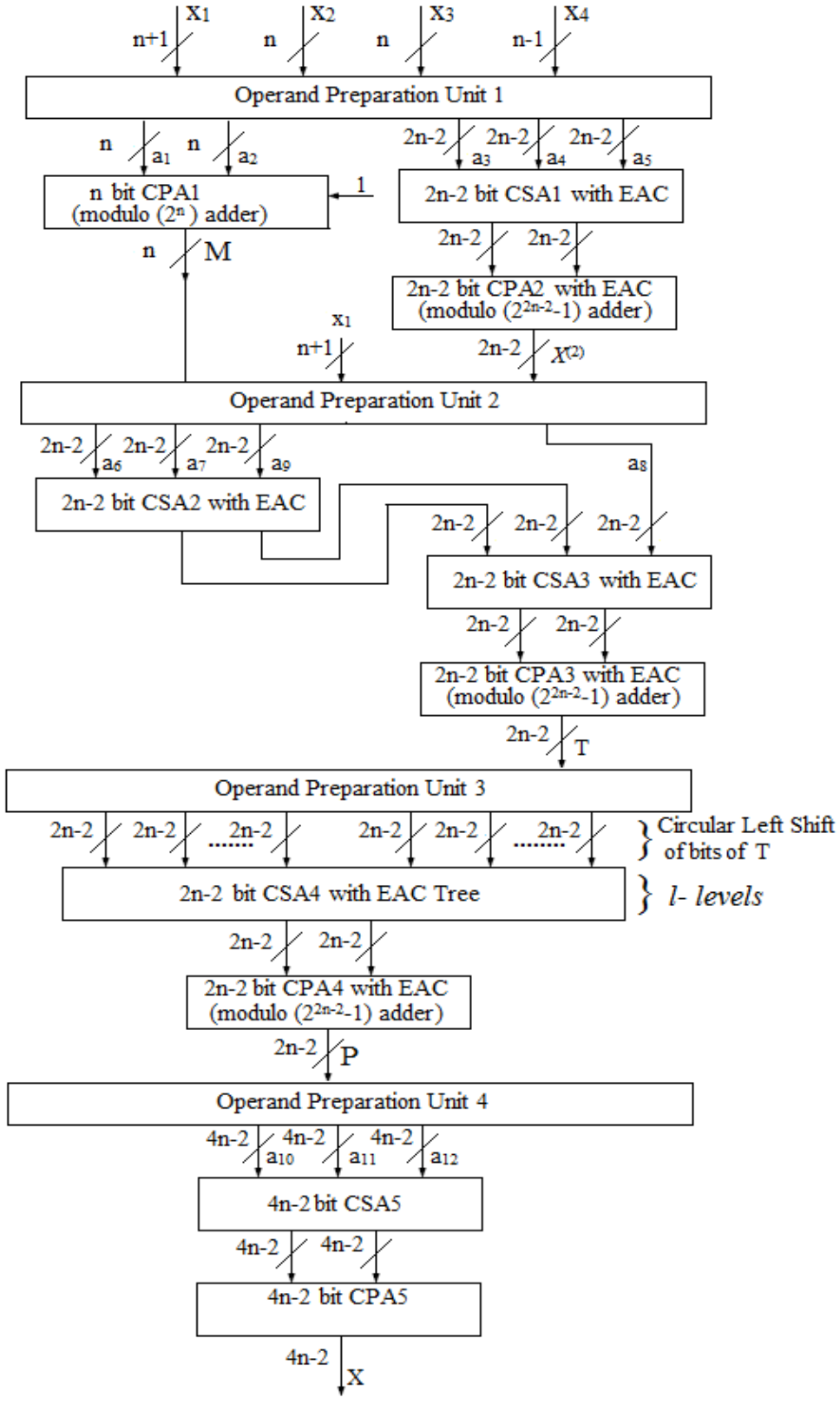


Figure 2.4 Reverse Converter for the moduli set P_1 using CRT and MRC

2.1.3 Reverse Converter Designs for $P_2 = \{2^{n-1}+1, 2^n-1, 2^n, 2^n+1\}$:

Consider the four moduli set $P_2 = \{2^{n-1}+1, 2^n, 2^n+1, 2^n-1\} = \{m_1, m_2, m_3, m_4\}$, where n is odd natural number (n>1) and let the corresponding residues of the integer *X* be (x_1, x_2, x_3, x_4). The residues have bit-level representations as:

$$x_1 = (x_{1,n-1}x_{1,n-2} \dots x_{1,1}x_{1,0})_2 \tag{2.116}$$

$$x_2 = (x_{2,n-1}x_{2,n-2} \dots x_{2,1}x_{2,0})_2 \tag{2.117}$$

$$x_3 = (x_{3,n}x_{3,n-1} \dots x_{3,1}x_{3,0})_2 \tag{2.118}$$

$$x_4 = (x_{4,n-1}x_{4,n-2} \dots x_{4,1}x_{4,0})_2 \tag{2.119}$$

The Sections 2.1.3.1 and 2.1.3.2 describe the design of reverse converters using different conversion algorithms.

2.1.3.1 Reverse Converter Design for P_2 Using New CRT II:

The value of *X* is calculated from New CRT II as follows:

$$X = Z + m_1 m_2 |k_1(Y - Z)|_{m_3 m_4} \tag{2.120}$$

where

$$Z = x_1 + m_1 \mid k_2(x_2 - x_1) \mid_{m_2} \tag{2.121}$$

$$Y = x_3 + m_3 \mid k_3(x_4 - x_3) \mid_{m_4} \tag{2.122}$$

$$k_1 = |(m_1 m_2)^{-1}|_{m_3 m_4},\ k_2 = |m_1^{-1}|_{m_2} \text{ and } k_3 = |m_3^{-1}|_{m_4} \tag{2.123}$$

The following propositions are needed for the derivation of *X*.

Proposition 1: The multiplicative inverse of $2^{n-1}+1$ modulo 2^n is:

$$|m_1^{-1}|_{m_2} = |(2^{n-1}+1)^{-1}|_{2^n} = 2^{n-1}+1 \tag{2.124}$$

where n is any odd number larger than 1.

Proof: The property of equation (1.35) defines if $|a^{-1}|_m = b$ then $|a \cdot b|_m = 1$

Since $|(2^{n-1}+1)^{-1}|_{2^n} = 2^{n-1}+1$, we have

$$|2^{n-1}+1\cdot 2^{n-1}+1|_{2^n} = |2^{2n-2}+2^n+1|_{2^n} = |0+0+1|_{2^n} = 1$$

Proposition 2: The multiplicative inverse of 2^n+1 modulo 2^n-1 is:

$$|m_3^{-1}|_{m_4} = |(2^n+1)^{-1}|_{2^n-1} = 2^{n-1} \tag{2.125}$$

where n is any odd number larger than 1.

Proof: Using inverse modulo property of equation (1.35).

Since $|(2^n+1)^{-1}|_{2^n-1} = 2^{n-1}$, we have

$$|(2^n+1)2^{n-1}|_{2^n-1} = |(2)2^{n-1}|_{2^n-1} = |2^n|_{2^n-1} = 1$$

Proposition 3: The multiplicative inverse of $(2^n\cdot 2^{n-1}+1)$ modulo $2^{2n}-1$ is:

$$|(m_1m_2)^{-1}|_{m_3m_4} = |(2^n\cdot 2^{n-1}+1)^{-1}|_{2^{2n}-1} = \sum_{l=2}^{n+1} 2^l + \sum_{m=n+2}^{2n-1} 2^m \tag{2.126}$$

where n is odd(n>1), *l* is even and m is odd. The above expression contains n terms.

Examples: The following values of multiplicative inverse for different values of n are found using the program given in Appendix A (Section A.2).

The value of $|(2^n\cdot 2^{n-1}+1)^{-1}|_{2^{2n}-1}$ for different values of n is:

For $n=3$, $|(2^n\cdot 2^{n-1}+1)^{-1}|_{2^{2n}-1} = |40^{-1}|_{63}$=52

$$= (110100)_2 \; in\; binary$$

$$= 2^2+2^4+2^5$$

$$= 2^2+2^{n+1}+2^{n+2}$$

For $n=5$, $|(2^n\cdot 2^{n-1}+1)^{-1}|_{2^{2n}-1} = |544^{-1}|_{1023}$=724

$$= (1011010100)_2$$

$$= 2^2+2^4+2^6+2^7+2^9$$

$$= 2^2+2^4+2^{n+1}+2^{n+2}+2^{2n-1}$$

For $n = 7, |(2^n \cdot 2^{n-1} + 1)^{-1}|_{2^{2n}-1} = |8320^{-1}|_{16383}$=11092

$$= (10101101010100)_2$$

$$= 2^2 + 2^4 + 2^6 + 2^8 + 2^9 + 2^{11} + 2^{13}$$

$$= 2^2 + 2^4 + 2^6 + 2^{n+1} + 2^{n+2} + 2^{n+4} + 2^{2n-1}$$

Thus the above values of $|(2^n \cdot 2^{n-1} + 1)^{-1}|_{2^{2n}-1}$ can be generalized as follows,

$$|(2^n \cdot 2^{n-1} + 1)^{-1}|_{2^{2n}-1} = \sum_{l=2}^{n+1} 2^l + \sum_{m=n+2}^{2n-1} 2^m \ , where\ l\ is\ even\ and\ m\ is\ odd$$

First, we simplify the equation (2.121) by substituting value of equation (2.124) as follows:

$$Z = x_1 + (2^{n-1} + 1) \mid (2^{n-1} + 1)(x_2 - x_1) \mid_{2^n} = x_1 + (2^{n-1} + 1)M \qquad (2.127)$$

where

$$M = |a_1 + a_2 + a_3 + a_4 + a_5|_{2^n} \qquad (2.128)$$

using properties of modulo (2^n) operator from Section 1.3.3, we have

$$a_1 = \underbrace{x_{2,0}}_{1} \underbrace{0 \dots 00}_{n-2} \underbrace{1}_{1} \qquad (2.129)$$

$$a_2 = \underbrace{\overline{x_{1,0}}}_{1} \underbrace{0 \dots 00}_{n-1} \qquad (2.130)$$

$$a_3 = \underbrace{1}_{1} \underbrace{0 \dots 00}_{n-1} \qquad (2.131)$$

$$a_4 = \underbrace{x_{2,n-1}x_{2,n-2} \dots x_{2,1}x_{2,0}}_{n} \qquad (2.132)$$

$$a_5 = \underbrace{\overline{x_{1,n-1}x_{1,n-2} \dots x_{1,1}x_{1,0}}}_{n} \qquad (2.133)$$

Next, the value of *Y* in equation (2.122) can be calculated from equations (2.21) to (2.26).

Finally, equation (2.120) can be simplified as

$$X = Z + 2^n(2^{n-1} + 1)|k_1(Y - Z)|_{2^{2n}-1} = Z + 2^n(2^{n-1} + 1)P \qquad (2.134)$$

where

$$P = |k_1 T|_{2^{2n}-1} \text{ and } T = |(Y - Z)|_{2^{2n}-1} \tag{2.135}$$

The value of T is simplified as:

$$T = |x_3 + (2^n + 1)N - x_1 - (2^{n-1} + 1)M|_{2^{2n}-1}$$

$$= |a_6 + a_7 + a_8 + a_9 + a_{10}|_{2^{2n}-1} \tag{2.136}$$

where

$$a_6 = \underbrace{0 \dots 00}_{n-1} \underbrace{x_{3,n} x_{3,n-1} \dots x_{3,1} x_{3,0}}_{n+1} \tag{2.137}$$

$$a_7 = \underbrace{N_{n-1} N_{n-2} \dots N_1 N_0}_{n} \underbrace{N_{n-1} N_{n-2} \dots N_1 N_0}_{n} \tag{2.138}$$

$$a_8 = \underbrace{1 \dots 11}_{n} \underbrace{\overline{x_{1,n-1} x_{1,n-2} \dots x_{1,1} x_{1,0}}}_{n} \tag{2.139}$$

$$a_9 = \underbrace{1}_{1} \underbrace{\overline{M_{n-1} M_{n-2} \dots M_1 M_0}}_{n} \underbrace{1 \dots 11}_{n-1} \tag{2.140}$$

$$a_{10} = \underbrace{1 \dots 11}_{n} \underbrace{\overline{M_{n-1} M_{n-2} \dots M_1 M_0}}_{n} \tag{2.141}$$

The value of *P* in equation (2.135) can be simplified by substituting value of equation (2.126) as:

$$P = |CLS(T, 2) + CLS(T, 4) + \cdots + CLS(T, n + 1) +$$

$$CLS(T, n + 2) + CLS(T, n + 4) \dots + CLS(T, 2n - 1)|_{2^{2n}-1} \tag{2.142}$$

The value of *X* in equation (2.134) can be simplified by substituting equation (2.127) as:

$$X = Z + 2^n(2^{n-1} + 1)P = x_1 + (2^{n-1} + 1)M + 2^n(2^{n-1} + 1)P$$

$$= x_1 + (2^{n-1} + 1)(M + 2^n P)$$

$$= x_1 + (2^{n-1} + 1)Q$$

$$= a_{11} + a_{12} + a_{13} \tag{2.143}$$

where

$$a_{11} = \underbrace{0 \dots 00}_{3n-1}\ \underbrace{x_{1,n-1}}_{1}\ \underbrace{0 \dots 00}_{n-1} \tag{2.144}$$

$$a_{12} = \underbrace{Q_{3n-1}Q_{3n-4} \dots Q_1Q_0}_{3n}\ \underbrace{x_{1,n-2}x_{1,n-3} \dots x_{1,1}x_{1,0}}_{n-1} \tag{2.145}$$

$$a_{13} = \underbrace{0 \dots 00}_{n-1}\ \underbrace{Q_{3n-1}Q_{3n-4} \dots Q_1Q_0}_{3n} \tag{2.146}$$

Example: Consider the moduli set $\{2^{n-1}+1, 2^n, 2^n+1, 2^n-1\}$ where n=3. The weighted number *X* can be calculated from its RNS representation (4, 7, 8, 6) as follows:

For n=3 the moduli set is {5, 8, 9, 7} and also residues have binary representation as below

$$x_1 = 4 = (100)_2$$

$$x_2 = 7 = (111)_2$$

$$x_3 = 8 = (1000)_2$$

$$x_4 = 6 = (110)_2$$

According to (2.129), (2.130), (2.131), (2.132), (2.133), (2.128), (2.22), (2.137), (2.138), (2.139), (2.140), (2.141), (2.136), and (2.142) we have

$$a_1 = (101)_2 = 5$$

$$a_2 = (100)_2 = 4$$

$$a_3 = (100)_2 = 4$$

$$a_4 = (111)_2 = 7$$

$$a_5 = (011)_2 = 3$$

$$M = |23|_8 = (111)_2 = 7$$

$$N = |(011)_2 + (011)_2|_7 = (110)_2 = 6$$

$$a_6 = (001000)_2 = 8$$

$$a_7 = (110110)_2 = 54$$

$$a_8 = (111011)_2 = 59$$

$$a_9 = (100011)_2 = 35$$

$$a_{10} = (111000)_2 = 56$$

$$T = |212|_{63} = 63 = (010111)_2$$

$$P = |125|_{63} = 62 = (111110)_2$$

Substituting the values *M* and *P* in *Q* and simplifying (2.144), (2.145), (2.146), *X* can be calculated from (2.143) as below:

$$a_{11} = (00000000100)_2 = 4$$

$$a_{12} = (11111011100)_2 = 2012$$

$$a_{13} = (00111110111)_2 = 503$$

$$X = 4 + 2012 + 503 = 2519$$

We can see that $|2519|_5 = 4$, $|2519|_8 = 7$, $|2519|_9 = 8$, $|2519|_7 = 6$, and therefore the calculated *X* is indeed the weighted value of the residue representation (4, 7, 8, 6) with respect to the moduli set {5, 8, 9, 7}.

Hardware Implementation: The reverse converter hardware architecture for the four moduli set $\{2^{n-1} + 1, 2^n, 2^n + 1, 2^n - 1\}$ with corresponding residues (x_1, x_2, x_3, x_4) of the integer *X* is shown in Fig. 2.5. Area and Delay specification for each part of the converter are shown in Table 2.6.

2.1.3.2 Reverse Converter Design for P_2 Using CRT and MRC:

The set P_2 is decomposed into two subsets $A_1 = \{2^{n-1} + 1, 2^n\}, A_2 = \{2^n + 1, 2^n - 1\}$. Two interim integers $X^{(1)}$ and $X^{(2)}$ are calculated from the residues x_1, x_2 of A_1 and x_3, x_4 of

Table 2.6

Area and Delay Specification of Reverse Converter for the moduli set P_2 using New CRT II

Parts	**FA**	**NOT**	**XOR/AND pairs**	**XNOR/OR pairs**	**MUX 2×1**	**Delay**
OPU 1		2n			1(n) -bit	$t_{NOT} + t_{MUX}$
CSA1	1		n-1			t_{FA}
CSA2	1		n-1			t_{FA}
CSA3	1		n-1			t_{FA}
CPA1	n					$n\ t_{FA}$
CPA2	n					$2n\ t_{FA}$
OPU2		2n				t_{NOT}
CSA4	2		n-1	n-1		t_{FA}
CSA5				n		t_{FA}
CSA6				n		t_{FA}
CPA3	2n					$4n\ t_{FA}$
OPU3	-					-
CSA7 Tree	$2n^2$-4n					$l \cdot t_{FA}$
CPA4	2n					$4n\ t_{FA}$
OPU4	-					-
CSA8	1		4n-2			t_{FA}
CPA5	4n-1					$(4n-1)t_{FA}$
Total Area		$(2n^2+6n+5)A_{FA}$+ (4n)A_{NOT}+ (8n-6)A_{XOR}+ (8n-6)A_{AND}+ (3n-1)A_{XNOR}+ (3n-1) A_{OR} + $A_{MUX(n)}$				
Total Delay		$(14n+3+l)t_{FA}$ + $2t_{NOT}$ + t_{MUX}				

Here *l* is the minimum number of levels of CSA tree required to process n input operands.

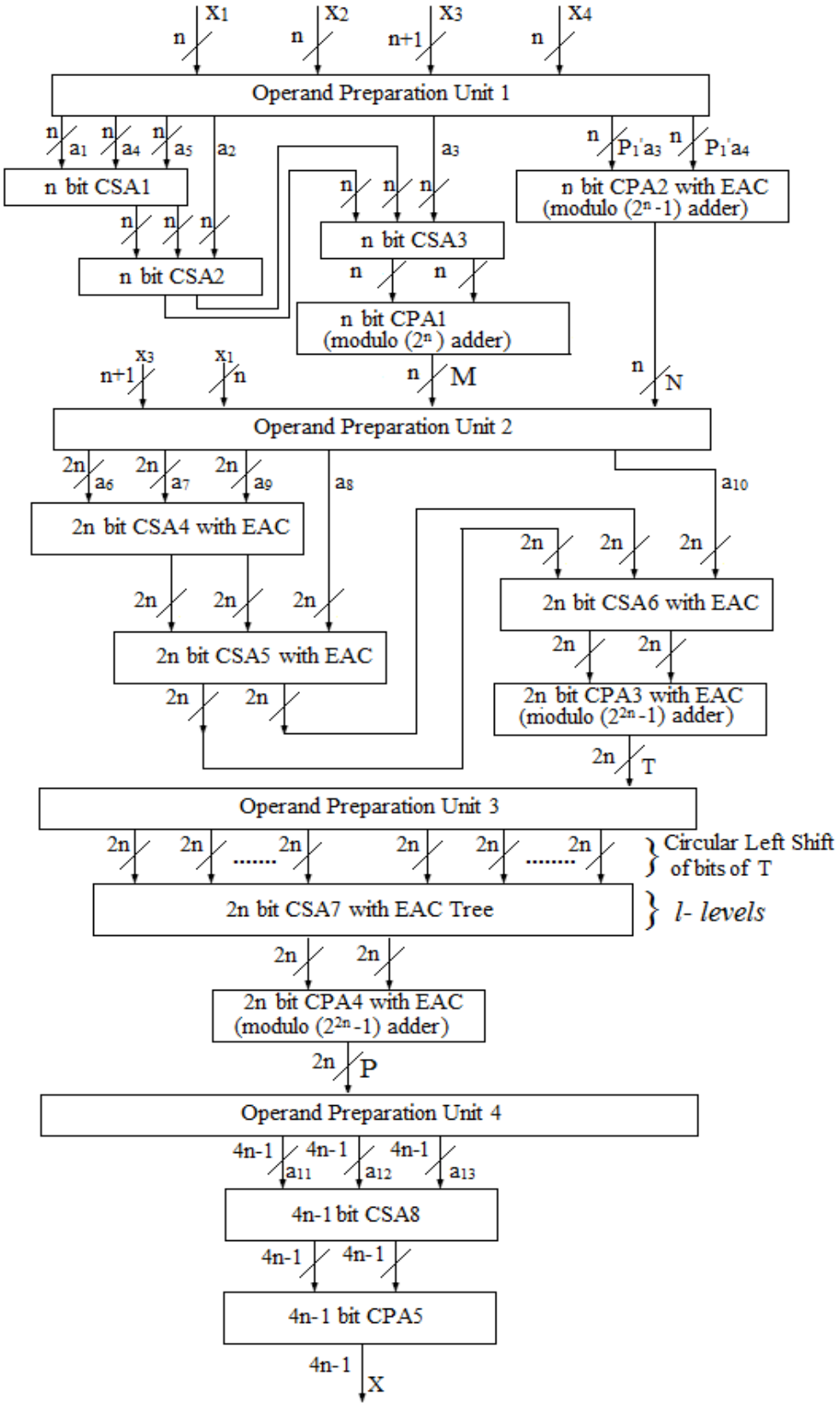


Figure 2.5 Reverse Converter for the moduli set P_2 using New CRT II

A_2 respectively. The conversion algorithms MRC and CRT are used to calculate $X^{(1)}$ and $X^{(2)}$ respectively. Next, the MRC algorithm is applied to calculate the final integer *X* from the residues ($X^{(1)},\ X^{(2)}$) corresponding to the moduli set $A_3 = \{2^n(2^{n-1}+1),\ (2^{2n}-1)\}$.

Calculation of $X^{(1)}$:

The value of $X^{(1)}$ is equal to Z in equation (2.127) and is calculated with the equations (2.128) to (2.133).

Calculation of $X^{(2)}$:

The value of $X^{(2)}$ is equal to $X^{(2)}$ in equation (2.49) and can be calculated using the equations (2.50) to (2.53) using CRT.

Calculation of X:

The value of *X* is calculated from MRC as follows:

$$X = X^{(1)} + 2^n(2^{n-1}+1)|k_1\left(X^{(2)} - X^{(1)}\right)|_{2^{2n}-1} = X^{(1)} + 2^n(2^{n-1}+1)P \qquad (2.147)$$

where

$$P = |k_1 T|_{2^{2n}-1} \text{ and } T = |\left(X^{(2)} - X^{(1)}\right)|_{2^{2n}-1} \qquad (2.148)$$

The value of T is simplified as:

$$\begin{aligned} T &= |X^{(2)} - x_1 - (2^{n-1}+1)M|_{2^{2n}-1} \\ &= |a_6 + a_7 + a_8 + a_9|_{2^{2n}-1} \end{aligned} \qquad (2.149)$$

where

$$a_6 = \underbrace{X_{2n-1}^{(2)} X_{2n-2}^{(2)} \dots X_1^{(2)} X_0^{(2)}}_{2n} \qquad (2.150)$$

$$a_7 = \underbrace{1 \dots 11}_{n}\ \underbrace{\overline{x_{1,n-1} x_{1,n-2} \dots x_{1,1} x_{1,0}}}_{n} \qquad (2.151)$$

$$a_8 = \underbrace{1}_{1}\underbrace{\overline{M_{n-1}M_{n-2}\dots M_1M_0}}_{n}\underbrace{1\dots 11}_{n-1} \tag{2.152}$$

$$a_9 = \underbrace{1\dots 11}_{n}\underbrace{\overline{M_{n-1}M_{n-2}\dots M_1M_0}}_{n} \tag{2.153}$$

The value of *P* in equation (2.148) can be simplified by substituting value of equation (2.126) as:

$$P = |CLS(T,2) + CLS(T,4) + \cdots + CLS(T,n+1) +$$
$$CLS(T,n+2) + CLS(T,n+4) \dots + CLS(T,2n-1)|_{2^{2n}-1} \tag{2.154}$$

The value of *X* in equation (2.147) can be simplified by substituting equation (2.127) as:

$$X = X^{(1)} + 2^n(2^{n-1}+1)P = x_1 + (2^{n-1}+1)M + 2^n(2^{n-1}+1)P$$
$$= x_1 + (2^{n-1}+1)(M + 2^nP)$$
$$= x_1 + (2^{n-1}+1)Q$$
$$= a_{10} + a_{11} + a_{12} \tag{2.155}$$

where

$$a_{10} = \underbrace{0\dots 00}_{3n-1}\underbrace{x_{1,n-1}}_{1}\underbrace{0\dots 00}_{n-1} \tag{2.156}$$

$$a_{11} = \underbrace{Q_{3n-1}Q_{3n-4}\dots Q_1Q_0}_{3n}\underbrace{x_{1,n-2}x_{1,n-3}\dots x_{1,1}x_{1,0}}_{n-1} \tag{2.157}$$

$$a_{12} = \underbrace{0\dots 00}_{n-1}\underbrace{Q_{3n-1}Q_{3n-4}\dots Q_1Q_0}_{3n} \tag{2.158}$$

Example: Consider the moduli set $\{2^{n-1}+1, 2^n, 2^n+1, 2^n-1\}$ where n=3. The weighted number *X* can be calculated from its RNS representation (2, 1, 6, 4) as follows:

For n=3 the moduli set is {5, 8, 9, 7} and also residues have binary representation as below

$$x_1 = 2 = (010)_2$$

$$x_2 = 1 = (001)_2$$

$$x_3 = 6 = (0110)_2$$

$$x_4 = 4 = (100)_2$$

According to (2.129), (2.130), (2.131), (2.132), (2.133), (2.128), (2.51), (2.52), (2.53), (2.50), (2.150), (2.151), (2.152), (2.153), (2.149), and (2.154) we have

$$a_1 = (101)_2 = 5$$

$$a_2 = (100)_2 = 4$$

$$a_3 = (100)_2 = 4$$

$$a_4 = (001)_2 = 1$$

$$a_5 = (101)_2 = 5$$

$$M = |19|_8 = (011)_2 = 3$$

$$X^{(2)} = |(000011)_2 + (010010)_2 + (100111)_2|_{63} = 60 = (111100)_2$$

$$a_6 = (111100)_2 = 60$$

$$a_7 = (111101)_2 = 61$$

$$a_8 = (110011)_2 = 51$$

$$a_9 = (111100)_2 = 60$$

$$T = |232|_{63} = 43 = (101011)_2$$

$$P = |2236|_{63} = 31 = (011111)_2$$

Substituting the values of *M* and *P* in *Q* and simplifying (2.156), (2.157), (2.158), *X* can be calculated from (2.155) as below

$$a_{10} = (00000000000)_2 = 0$$

$$a_{11} = (01111101110)_2 = 1006$$

$$a_{12} = (00011111011)_2 = 251$$

$$X = 0 + 1006 + 251 = 1257$$

We can see that $|1257|_5 = 2$, $|1257|_8 = 1$, $|1257|_9 = 6$, $|1257|_7 = 4$, and therefore the calculated *X* is indeed the weighted value of the residue representation (2, 1, 6, 4) with respect to the moduli set {5, 8, 9, 7}.

Hardware Implementation: The reverse converter hardware architecture for the four moduli set $\{2^{n-1}+1, 2^n, 2^n+1, 2^n-1\}$ with corresponding residues (x_1, x_2, x_3, x_4) of the integer *X* is shown in Fig. 2.6. Area and Delay specification for each part of the converter are shown in Table 2.7.

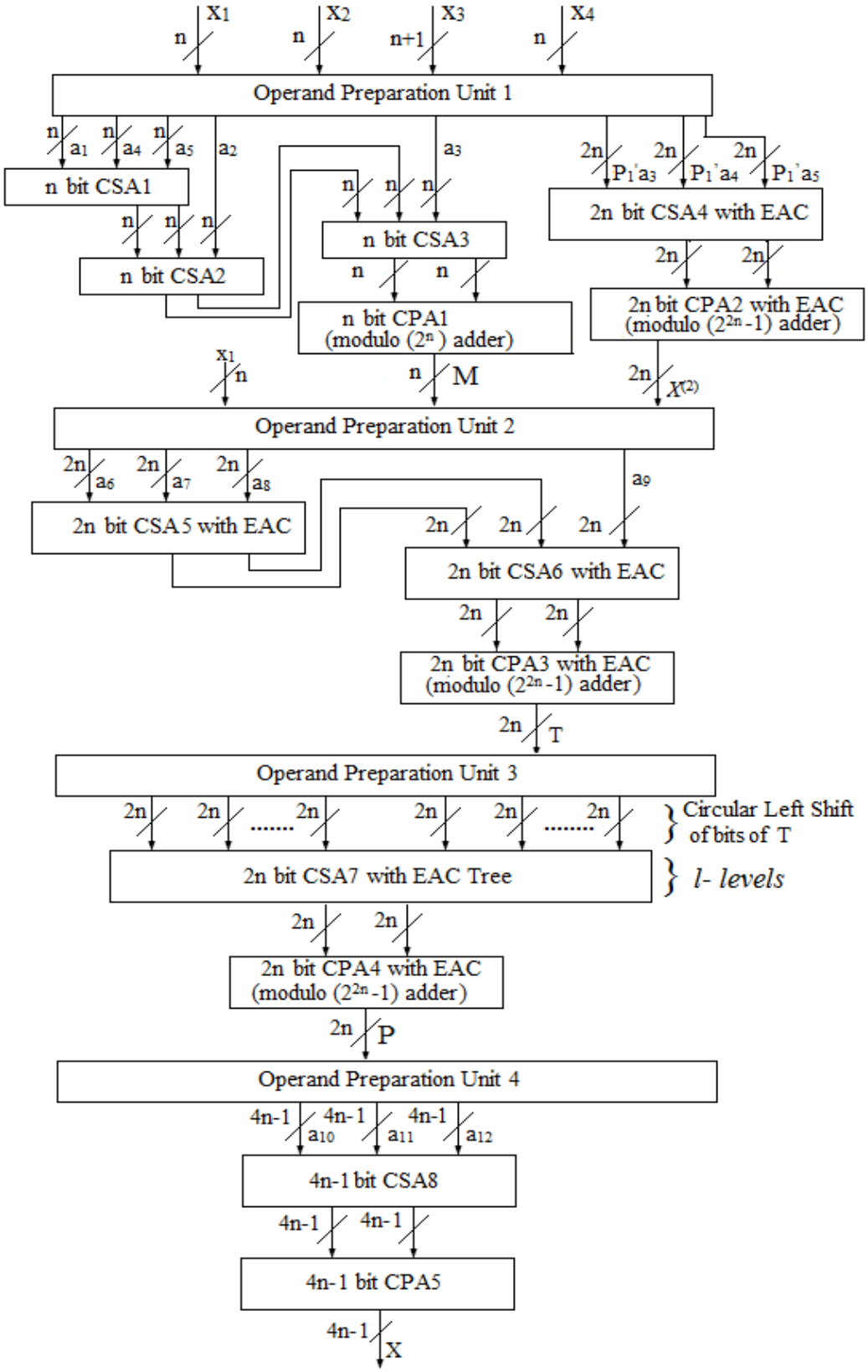


Figure 2.6 Reverse Converter for the moduli set P_2 using CRT and MRC

Table 2.7

Area and Delay Specification of Reverse Converter for the moduli set P_2 using CRT and MRC

Parts	**FA**	**NOT**	**XOR/AND pairs**	**XNOR/OR pairs**	**Delay**
OPU 1		2n			t_{NOT}
CSA1	1		n-1		t_{FA}
CSA2	1		n-1		t_{FA}
CSA3	1		n-1		t_{FA}
CPA1	n				$n\ t_{FA}$
CSA4	2		n-1	n-1	t_{FA}
CPA2	2n				$4n\ t_{FA}$
OPU2		2n			t_{NOT}
CSA5	1			2n-1	t_{FA}
CSA6	n			n	t_{FA}
CPA3	2n				$4n\ t_{FA}$
OPU3	-				-
CSA7 Tree	$2n^2$-4n				$l \cdot t_{FA}$
CPA4	2n				$4n\ t_{FA}$
OPU4	-				-
CSA8	1		4n-2		t_{FA}
CPA5	4n-1				$(4n-1)t_{FA}$
Total Area		$(2n^2+8n+6)A_{FA}+(4n)A_{NOT}+(8n-6)A_{XOR}+(8n-6)A_{AND}+(4n-2)A_{XNOR}+(4n-2)\ A_{OR}$			
Total Delay		$(16n+3+l)t_{FA}+2t_{NOT}$			

Here *l* is the minimum number of levels of CSA tree required to process n input operands.

3. DESIGN OF REVERSE CONVERTERS FOR FIVE MODULI SETS

3.1 Five Moduli Sets:

The efficiency of Residue Number System depends not only on the residue to binary converter but also on the operand sizes and modulus in each residue channel. In order to implement fast RNS systems for a given dynamic range, (or alternatively speaking to implement large dynamic ranges without slowing-down the internal RNS processing), multi-moduli RNS systems with many small moduli must be considered. Thus the four moduli sets are extended to form five moduli sets, and this extension increases the parallelism and reduces the size of each residue channel for a given dynamic range.

The five moduli sets P_3 , P_4 and four moduli set P_1' shown below have been proposed by Abdallah and Skavantzos in [18] for radix r. In this research, a new group of five moduli sets S_1 to S_6 shown below have been proposed by modifying the five moduli sets P_3 , P_4 and extending the four moduli set P_1'. The reverse converters for these new five moduli sets have been designed for binary domain, i.e. for radix r=2. The main idea behind modifying the moduli sets proposed in [18] is to simplify the design of reverse converters using modulo (2^n) and modulo ($2^n - 1$) adders. Also, the importance of these moduli sets is that they contain the moduli of the form 2^a, $2^b - 1$, $2^c + 1$ (a, b and c are natural numbers) which can be efficiently implemented using usual binary hardware that leads to simple design and offers speed-cost benefits. The reverse converters are designed by applying any one or combination of two or more conversion algorithms discussed in Section 1.2.4.

The four and five moduli sets P_1', P_3 , P_4 proposed in [18] are:

$$P_1' = \{2^{n-1} - 1, 2^n - 1, 2^n, 2^n + 1\}, \text{where } n = 2k, k = 2, 3, 4, \ldots \quad (3.1)$$

$$P_3 = \{2^{n-2}+1, 2^{n-1}-1, 2^{n-1}+1, 2^n, 2^n+1\}, \text{where } n = 2k, k = 2, 3, 4, \ldots \quad (3.2)$$

$$P_4 = \{2^{n-2}-1, 2^{n-1}+1, 2^n-1, 2^n, 2^n+1\}, \text{where } n = 2k+1, k = 2, 3, 4, \ldots \quad (3.3)$$

The new five moduli sets proposed in this research are:

$$S_1 = \{2^{2n-2}+1, 2^{n-1}-1, 2^{n-1}+1, 2^n, 2^{2n}+1\}, \text{where } n = 2k, k = 2, 3, 4, \ldots \quad (3.4)$$

$$S_2 = \{2^{2n-1}-1, 2^{n-1}-1, 2^n-1, 2^n, 2^n+1\}, \text{where } n = 2k, k = 2, 3, 4, \ldots \quad (3.5)$$

$$S_3 = \{2^{2n-1}-1, 2^{2n}+1, 2^n-1, 2^n, 2^n+1\}, \text{where } n = 2, 3, 4, \ldots \quad (3.6)$$

$$S_4 = \{2^{2n-1}-1, 2^{2n}+1, 2^n-1, 2^{2n}, 2^n+1\}, \text{where } n = 2, 3, 4, \ldots \quad (3.7)$$

$$S_5 = \{2^{4n}+1, 2^{2n}+1, 2^n-1, 2^n, 2^n+1\}, \text{where } n = 3, 4, 5 \ldots \quad (3.8)$$

$$S_6 = \{2^{4n}+1, 2^{2n}+1, 2^n-1, 2^{2n}, 2^n+1\}, \text{where } n = 2, 3, 4 \ldots \quad (3.9)$$

The proof for the new five moduli sets to be pairwise relatively prime is given in Appendix B. The following sections describe the design of reverse converters for the new five moduli sets.

3.1.1 Reverse Converter Design for $S_1 = \{2^{2n-2}+1, 2^{n-1}-1, 2^{n-1}+1, 2^n, 2^{2n}+1\}$:

Consider the five moduli set $S_1 = \{2^{2n-2}+1, 2^{n-1}-1, 2^{n-1}+1, 2^n, 2^{2n}+1\} = \{m_1, m_2, m_3, m_4, m_5\}$, where n is even natural number (n>2) and let the corresponding residues of the integer *X* be $(x_1, x_2, x_3, x_4, x_5)$. The residues have bit-level representations as:

$$x_1 = (x_{1,2n-2}x_{1,2n-3} \ldots x_{1,1}x_{1,0})_2 \quad (3.10)$$

$$x_2 = (x_{2,n-2}x_{2,n-3} \ldots x_{2,1}x_{2,0})_2 \quad (3.11)$$

$$x_3 = (x_{3,n-1}x_{3,n-2} \ldots x_{3,1}x_{3,0})_2 \quad (3.12)$$

$$x_4 = (x_{4,n-1}x_{4,n-2} \ldots x_{4,1}x_{4,0})_2 \quad (3.13)$$

$$x_5 = (x_{5,2n}x_{5,2n-1} \ldots x_{5,1}x_{5,0})_2 \quad (3.14)$$

The following section describes the design of reverse converter for S_1 using New CRT I and MRC conversion algorithms.

3.1.1.1 Reverse Converter Design for S_1 Using New CRT I and MRC:

The set S_1 here is decomposed into two subsets $A_1 = \{2^{2n-2}+1, 2^{n-1}-1, 2^{n-1}+1\}$ and $A_2 = \{2^n, 2^{2n}+1\}$. Two interim integers Y and Z are calculated from the residues x_1, x_2, x_3 of A_1 and x_4, x_5 of A_2 respectively. The conversion algorithms New CRT I and MRC are used to calculate Y and Z respectively. Next, the MRC algorithm is applied to calculate the final integer X from the residues $(Z,\ Y)$ corresponding to the moduli set $A_3 = \{2^n(2^{2n}+1), 2^{4n-4}-1\}$. The following propositions are needed for the derivation of X.

Proposition 1: The multiplicative inverse of $2^{2n-2}+1$ modulo $2^{2n-2}-1$ is:

$$|m_1^{-1}|_{m_2 m_3} = |(2^{2n-2}+1)^{-1}|_{2^{2n-2}-1} = 2^{2n-3} \tag{3.15}$$

where n is any even number larger than 2.

Proof: Using property of equation (1.35), if $|a^{-1}|_m = b$ then $|a \cdot b|_m = 1$

Since $|(2^{2n-2}+1)^{-1}|_{2^{2n-2}-1} = 2^{2n-3}$, we have

$$|2^{2n-2} + 1 \cdot 2^{2n-3}|_{2^{2n-2}-1} = |2 \cdot 2^{2n-3}|_{2^{2n-2}-1} = |2^{2n-2}|_{2^{2n-2}-1} = 1$$

Proposition 2: The multiplicative inverse of $(2^{2n-2}+1)(2^{n-1}-1)$ modulo $2^{n-1}+1$ is:

$$|(m_1 m_2)^{-1}|_{m_3} = |((2^{2n-2}+1)(2^{n-1}-1))^{-1}|_{2^{n-1}+1} = 2^{n-3} \tag{3.16}$$

where n is any even number larger than 2.

Proof: Using property of equation (1.35), if $|a^{-1}|_m = b$ then $|a \cdot b|_m = 1$

Since $|((2^{2n-2}+1)(2^{n-1}-1))^{-1}|_{2^{n-1}+1} = 2^{n-3}$, we have

$$|(2^{2n-2}+1)(2^{n-1}-1)2^{n-3}|_{2^{n-1}+1} = |(2)(-2) \cdot 2^{n-3}|_{2^{n-1}+1} = |-2^{n-1}|_{2^{n-1}+1} = 1$$

Proposition 3: The multiplicative inverse of $(2^{2n}+1)$ modulo 2^n is:

$$|(m_5)^{-1}|_{m_4} = |(2^{2n}+1)^{-1}|_{2^n} = 1 \tag{3.17}$$

where n is any even number larger than 2.

Proof: Using property of equation (1.35), if $|a^{-1}|_m = b$ then $|a \cdot b|_m = 1$

Since $|(2^{2n}+1)^{-1}|_{2^n} = 1$, we have $|2^{2n}+1|_{2^{2n}} = 1$

Proposition 4: The multiplicative inverse of $(2^n \cdot 2^{2n}+1)$ modulo $2^{4n-4}-1$ is:

$$|(m_4 m_5)^{-1}|_{m_1 m_2 m_3} = |(2^n \cdot 2^{2n}+1)^{-1}|_{2^{4n-4}-1}$$

$$= \begin{cases} \sum_{l=3}^{n-1} 2^l + \sum_{m=n}^{3n-6} 2^m + \sum_{i=3n-1}^{4n-5} 2^i & if\ n = 4k, k = 1,2,3 \ldots \\ \sum_{l=1}^{n-1} 2^l + \sum_{m=n}^{3n-6} 2^m + \sum_{i=3n-1}^{4n-7} 2^i & if\ n = 4k+2, k = 1,2,3 \ldots \end{cases} \quad (3.18)$$

where n is even(n>2), *l* is odd, m is natural number (m≠ n+2j+1 where j=1,3,5….), *i* is odd. The above expression contains $(2n-3)$ terms.

Examples: The following values of multiplicative inverse for different values of n are found using the program given in Appendix A (Section A.2).

The value of $|(2^n \cdot 2^{2n}+1)^{-1}|_{2^{4n-4}-1}$ for different values of n is:

For $n = 4$, $|(2^n \cdot 2^{2n}+1)^{-1}|_{2^{4n-4}-1} = |4112^{-1}|_{4095}$=2168

$= (100001111000)_2\ in\ binary$

$= 2^3 + 2^4 + 2^5 + 2^6 + 2^{11}$

For $n = 6$, $|(2^n \cdot 2^{2n}+1)^{-1}|_{2^{4n-4}-1} = |262208^{-1}|_{1048575}$=138722

$= (100001110111100010)_2$

$= 2^1 + 2^5 + 2^6 + 2^7 + 2^8 + 2^{10} + 2^{11} + 2^{12} + 2^{17}$

For $n = 8$, $|(2^n \cdot 2^{2n}+1)^{-1}|_{2^{4n-4}-1} = |16777472^{-1}|_{268435455}$=143095688

$= (10001000011101110111100010 00)_2$

$= 2^3 + 2^7 + 2^8 + 2^9 + 2^{10} + 2^{12} + 2^{13} + 2^{14} + 2^{16} + 2^{17} + 2^{18} + 2^{23} + 2^{27}$

For $n = 10$, $|(2^n \cdot 2^{2n}+1)^{-1}|_{2^{4n-4}-1} = |1073742848^{-1}|_{68719476735}$=9158123042

$= (10001000011101110111011110001000 10)_2$

$$= 2^1 + 2^5 + 2^9 + 2^{10} + 2^{11} + 2^{12} + 2^{14} + 2^{15} + 2^{16} + 2^{18} + 2^{19} + 2^{20} + 2^{22} + 2^{23} + 2^{24} + 2^{29} + 2^{33}$$

Thus the above values of $|(2^n \cdot 2^{n-1} - 1)^{-1}|_{2^{2n}-1}$ can be generalized as follows,

$$|(2^n \cdot 2^{2n} + 1)^{-1}|_{2^{4n-4}-1} = \begin{cases} \sum_{l=3}^{n-1} 2^l + \sum_{m=n}^{3n-6} 2^m + \sum_{i=3n-1}^{4n-5} 2^i & if\ n = 4k, k = 1,2,3 \dots \\ \sum_{l=1}^{n-1} 2^l + \sum_{m=n}^{3n-6} 2^m + \sum_{i=3n-1}^{4n-7} 2^i & if\ n = 4k+2, k = 1,2,3 \dots \end{cases}$$

where n is even(n>2), l is odd($l \neq$ 4p+1 for $n = 4k$ and $l \neq$ 4p -1 for $n = 4k + 2$ where p=1,2,3…), m is a natural number (m≠ n+2j+1 where j=1,3,5….), i is odd.

Calculation of Y:

The value of Y is calculated from New CRT I as follows:

$$Y = x_1 + m_1 \cdot | \ |m_1^{-1}|_{m_2 m_3} \cdot (x_2 - x_1) + |(m_1 m_2)^{-1}|_{m_3} \cdot m_2 \cdot (x_3 - x_2) \ |_{m_2 m_3} \qquad (3.19)$$

Substituting the value (3.15), (3.16), m_1, m_2 and m_3 in (3.19) we have

$$Y = x_1 + (2^{2n-2} + 1)|2^{2n-3} \cdot (x_2 - x_1) + 2^{n-3}(2^{n-1} - 1)(x_3 - x_2) \ |_{2^{2n-2}-1}$$

$$= x_1 + (2^{2n-2} + 1)M \qquad (3.20)$$

where

$$M = | \ a_1 + a_2 + a_3 + a_4 \ |_{2^{2n-2}-1} \qquad (3.21)$$

$$a_1 = \underbrace{x_{2,1}x_{2,0}}_{2} \underbrace{x_{2,n-2}x_{2,n-3} \dots x_{2,1}x_{2,0}}_{n-1} \underbrace{x_{2,n-2}x_{2,n-3} \dots x_{2,2}}_{n-3} \qquad (3.22)$$

$$a_2 = \begin{cases} a_{21} & if\ x_{1,2n-2} = 1 \\ a_{22} & if\ x_{1,2n-2} = 0 \end{cases} \qquad (3.23)$$

$$a_{21} = \underbrace{0}_{1} \underbrace{1 \dots 11}_{2n-3} \qquad (3.24)$$

$$a_{22} = \underbrace{\overline{x_{1,0}x_{1,2n-3} \dots x_{1,2}x_{1,1}}}_{2n-2} \qquad (3.25)$$

$$a_3 = \underbrace{x_{3,1}x_{3,0}}_{2}\ \underbrace{0\ldots00}_{n-2}\ \underbrace{x_{3,n-1}x_{3,n-2}\ldots x_{3,2}}_{n-2} \tag{3.26}$$

$$a_4 = \underbrace{1}_{1}\ \underbrace{\overline{x_{3,n-1}x_{3,n-2}\ldots x_{3,1}x_{3,0}}}_{n}\ \underbrace{1\ldots11}_{n-3} \tag{3.27}$$

Calculation of Z:

The value of Z is calculated from MRC as follows:

$$Z = x_5 + m_5 \cdot |\ |m_5^{-1}|_{m_4} \cdot (x_4 - x_5)|_{m_4} \tag{3.28}$$

Substituting the value (3.17), m_4, and m_5 in (3.28) we have

$$\begin{aligned} Z &= x_5 + (2^{2n}+1)|1 \cdot (x_4 - x_5)|_{2^n} \\ &= x_5 + (2^{2n}+1)N \end{aligned} \tag{3.29}$$

where

$$N = |a_5 + a_6|_{2^n} \tag{3.30}$$

$$a_5 = \underbrace{x_{4,n-1}x_{4,n-2}\ldots x_{4,1}x_{4,0}}_{n} \tag{3.31}$$

$$a_6 = \underbrace{\overline{x_{5,n-1}x_{5,n-2}\ldots x_{5,1}x_{5,0}}}_{n} \quad (+1 \text{ as Carry in to CPA}) \tag{3.32}$$

Now the value of *X* is calculated from MRC as follows:

$$\begin{aligned} X &= Z + 2^n(2^{2n}+1)||(2^n \cdot 2^{2n}+1)^{-1}|_{2^{4n-4}-1} \cdot (Y - Z)|_{2^{4n-4}-1} \\ &= Z + 2^n(2^{2n}+1)P \end{aligned} \tag{3.33}$$

where

$$P = ||(2^n \cdot 2^{2n}+1)^{-1}|_{2^{4n-4}-1}T|_{2^{4n-4}-1} \text{ and } T = |(Y - Z)|_{2^{4n-4}-1} \tag{3.34}$$

$$\begin{aligned} T &= |(Y - Z)|_{2^{4n-4}-1} = |x_1 + (2^{2n-2}+1)M - x_5 - (2^{2n}+1)N|_{2^{4n-4}-1} \\ &= |a_7 + a_8 + a_9 + a_{10}|_{2^{4n-4}-1} \end{aligned} \tag{3.35}$$

$$a_7 = \underbrace{0\ldots00}_{2n-3}\ \underbrace{x_{1,2n-2}x_{1,2n-3}\ldots x_{1,1}x_{1,0}}_{2n-1} \tag{3.36}$$

$$a_8 = \underbrace{M_{2n-3}M_{2n-4}\dots M_1M_0}_{2n-2}\,\underbrace{M_{2n-3}M_{2n-4}\dots M_1M_0}_{2n-2} \tag{3.37}$$

$$a_9 = \underbrace{1\dots11}_{2n-5}\,\underbrace{\overline{x_{5,2n}x_{5,2n-1}\dots x_{5,1}x_{5,0}}}_{2n+1} \tag{3.38}$$

$$a_{10} = \underbrace{1\dots11}_{n-4}\,\underbrace{\overline{N_{n-1}N_{n-2}\dots N_1N_0}}_{n}\,\underbrace{1\dots11}_{n}\,\underbrace{\overline{N_{n-1}N_{n-2}\dots N_1N_0}}_{n} \tag{3.39}$$

The value of *P* in equation (3.34) can be simplified by substituting value of equation (3.18) and operating circular left shift on bits of *T*.

The value of *X* in equation (3.33) can be simplified by substituting equation (3.29) as:

$$X = Z + 2^n(2^{2n}+1)P = x_5 + (2^{2n}+1)N + 2^n(2^{2n}+1)P$$

$$= x_5 + (2^{2n}+1)(N + 2^nP)$$

$$= x_5 + (2^{2n}+1)Q$$

$$= a_{11} + a_{12} + a_{13} \tag{3.40}$$

where

$$a_{11} = \underbrace{0\dots00}_{5n-5}\,\underbrace{x_{5,2n}}_{1}\,\underbrace{0\dots00}_{2n} \tag{3.41}$$

$$a_{12} = \underbrace{Q_{5n-5}Q_{5n-6}\dots Q_1Q_0}_{5n-4}\,\underbrace{x_{5,2n-1}x_{5,2n-2}\dots x_{5,1}x_{5,0}}_{2n} \tag{3.42}$$

$$a_{13} = \underbrace{0\dots00}_{2n}\,\underbrace{Q_{5n-5}Q_{5n-6}\dots Q_1Q_0}_{5n-4} \tag{3.43}$$

Example: Consider the moduli set $\{2^{2n-2}+1, 2^{n-1}-1, 2^{n-1}+1, 2^n, 2^{2n}+1\}$ where n=4. The weighted number *X* can be calculated from its RNS representation (1, 6, 4, 5, 177) as follows:

For n=4 the moduli set is {65, 7, 9, 16, 257} and also residues have binary representation as below

$$x_1 = 1 = (0000001)_2$$

$$x_2 = 6 = (110)_2$$

$$x_3 = 4 = (0100)_2$$

$$x_4 = 5 = (0101)_2$$

$$x_5 = 177 = (010110001)_2$$

According to (3.22), (3.23), (3.26), (3.27), (3.21), (3.31), (3.32), (3.30), (3.36), (3.37), (3.38), (3.39), (3.35), and (3.34) we have

$$a_1 = (101101)_2 = 45$$

$$a_2 = a_{22} = (011111)_2 = 31$$

$$a_3 = (000001)_2 = 1$$

$$a_4 = (110111)_2 = 55$$

$$M = |132|_{63} = (000110)_2 = 6$$

$$a_5 = (0101)_2 = 5$$

$$a_6 = (1110)_2(+1\ as\ carry\ in) = 15$$

$$T = |20|_{16} = 4 = (0100)_2$$

$$a_7 = (000000000001)_2 = 1$$

$$a_8 = (000110000110)_2 = 390$$

$$a_9 = (111101001110)_2 = 51$$

$$a_{10} = (101111111011)_2 = 3067$$

$$T = |3509|_{4095} = 3281 = (110011010001)_2$$

$$P = |12478|_{4095} = 193 = (11000001)_2$$

Substituting the values of *N* and *P* in *Q* and simplifying (3.41), (3.42), (3.43), *X* can be calculated from (3.40) as below

$$a_{11} = (000000000000000000000000)_2 = 0$$

$$a_{12} = (000011000001010010110001)_2 = 791729$$

$$a_{13} = (000000000000110000010100)_2 = 3092$$

$$X = 0 + 791729 + 3092 = 794821$$

We can see that $|794821|_{65} = 1$, $|794821|_7 = 6$, $|794821|_9 = 4$, $|794821|_8 = 5$, $|794821|_{257} = 177$ and therefore the calculated *X* is indeed the weighted value of the residue representation (1, 6, 4, 5, 177) with respect to the moduli set {65, 7, 9, 16, 257}.

Hardware Implementation: The reverse converter hardware architecture for the five moduli set $\{2^{2n-2}+1, 2^{n-1}-1, 2^{n-1}+1, 2^n, 2^{2n}+1\}$ with corresponding residues $(x_1, x_2, x_3, x_4, x_5)$ of the integer *X* is shown in Fig. 3.1. Area and Delay specification for each part of the converter are shown in Table 3.1.

3.1.2 Reverse Converter Design for $S_2 = \{2^{2n-1}-1, 2^{n-1}-1, 2^n-1, 2^n, 2^n+1\}$:

Consider the five moduli set $S_2 = \{2^n-1, 2^n, 2^n+1, 2^{n-1}-1, 2^{2n-1}-1\} = \{m_1, m_2, m_3, m_4, m_5\}$, where n is even natural number (n>2) and let the corresponding residues of the integer *X* be $(x_1, x_2, x_3, x_4, x_5)$. The residues have bit-level representations as:

$$x_1 = (x_{1,n-1}x_{1,n-2} \dots x_{1,1}x_{1,0})_2 \quad (3.44)$$

$$x_2 = (x_{2,n-1}x_{2,n-2} \dots x_{2,1}x_{2,0})_2 \quad (3.45)$$

$$x_3 = (x_{3,n}x_{3,n-1} \dots x_{3,1}x_{3,0})_2 \quad (3.46)$$

$$x_4 = (x_{4,n-2}x_{4,n-3} \dots x_{4,1}x_{4,0})_2 \quad (3.47)$$

$$x_5 = (x_{5,2n-2}x_{5,2n-3} \dots x_{5,1}x_{5,0})_2 \quad (3.48)$$

The following section describes the design of reverse converter for S_2 using New CRT I and MRC conversion algorithms.

Table 3.1

Area and Delay Specification of Reverse Converter for the moduli set S_1 using New CRT I and MRC

Parts	**FA**	**NOT**	**XOR/AND pairs**	**XNOR/OR pairs**	**Delay**
OPU 1		4n-2			t_{NOT}
CSA1	n		n-2		t_{FA}
CSA2	n			n-2	t_{FA}
CPA1	2n-2				$(4n-4)t_{FA}$
CPA2	n				$n\ t_{FA}$
OPU2		3n+1			t_{NOT}
CSA3	2n-1		2n-3		t_{FA}
CSA4	2n			2n-4	t_{FA}
CPA3	4n-4				$(8n-8)t_{FA}$
OPU3	-				-
CSA5 Tree	$8n^2$-28n+20				$l \cdot t_{FA}$
CPA4	4n-4				$(8n-8)t_{FA}$
OPU4	-				-
CSA6	1		7n-5		t_{FA}
CPA5	7n-4				$(7n-4)t_{FA}$
Total Area		$(8n^2$ -4n+6)A_{FA}+ (7n-1)A_{NOT}+ (10n-10)A_{XOR}+ (10n-10)A_{AND}+ (3n-6)A_{XNOR}+ (3n-6) A_{OR}			
Total Delay		$(27n-19+l)t_{FA}$ + $2t_{NOT}$			

Here *l* is the minimum number of levels of CSA tree required to process 2n-3 input operands.

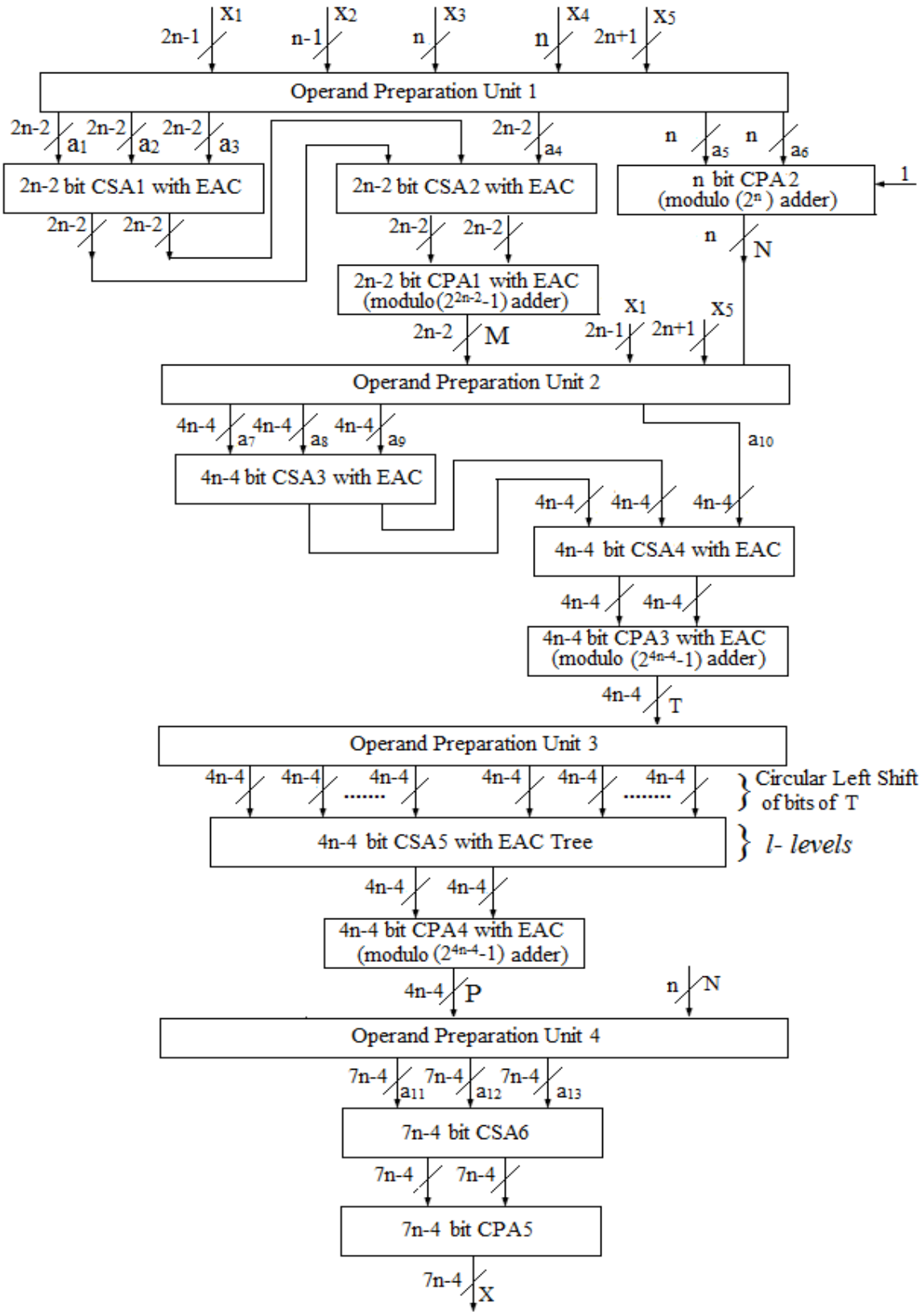


Figure 3.1 Reverse Converter for the moduli set S_1 using New CRT I and MRC

3.1.2.1 Reverse Converter Design for S_2 Using New CRT I and MRC:

The set S_2 here is decomposed into two subsets $A_1 = \{2^n - 1, 2^n, 2^n + 1, 2^{n-1} - 1\}$ and $A_2 = \{2^{2n-1} - 1\}$. An integer $X^{(1)}$ is calculated from the residues x_1, x_2, x_3, x_4 of A_1. The conversion algorithms New CRT I and MRC are used to calculate $X^{(1)}$. Next, the MRC algorithm is applied to calculate the integer *X* from the residues $(X^{(1)}, x_5)$ corresponding to the moduli set $A_3 = \{2^n(2^{2n} - 1)(2^{n-1} - 1), 2^{2n-1} - 1\}$. The following proposition is needed for the derivation of *X*.

Proposition 1: The multiplicative inverse of $2^n(2^{2n} - 1)(2^{n-1} - 1)$ modulo $2^{2n-1} - 1$ is:

$$|(2^n(2^{2n} - 1)(2^{n-1} - 1))^{-1}|_{2^{2n-1}-1} = 2^{2n-1} - 2^n - 2 \tag{3.49}$$

where n is any even number larger than 2.

Proof: Using property of equation (1.35), if $|a^{-1}|_m = b$ then $|a \cdot b|_m = 1$

Since $|(2^n(2^{2n} - 1)(2^{n-1} - 1))^{-1}|_{2^{2n-1}-1} = 2^{2n-1} - 2^n - 2$, we have

$$|2^n(2^{2n} - 1)(2^{n-1} - 1)(2^{2n-1} - 2^n - 2)|_{2^{2n-1}-1}$$

$$= |2^n(2 - 1)(2^{n-1} - 1)(1 - 2^n - 2)|_{2^{2n-1}-1}$$

$$= |(2^{2n-1} - 2^n)(-2^n - 1)|_{2^{2n-1}-1} = |(2^n - 1)(2^n + 1)|_{2^{2n-1}-1}$$

$$= |(2^{2n} - 1)|_{2^{2n-1}-1} = |(2.2^{2n-1} - 1)|_{2^{2n-1}-1} = 1$$

Calculation of $X^{(1)}$:

The converter design and proof for calculation of value of $X^{(1)}$ for four moduli set $\{2^n - 1, 2^n, 2^n + 1, 2^{n-1} - 1\}$ using New CRT I and MRC is given in [19]. The hardware and delay specification for this converter are given in section 2.1.1.3. The following equation from [19] is useful for the derivation of *X*.

$$X^{(1)} = x_2 + 2^n(2^{2n}Z + Y - Z) = x_2 + 2^nK \tag{3.50}$$

Calculation of X:

The value of X is calculated from MRC as shown below:

$$X = X^{(1)} + 2^n(2^{2n}-1)(2^{n-1}-1)||(2^n(2^{2n}-1)(2^{n-1}-1))^{-1}|_{2^{2n-1}-1}(x_5 - X^{(1)})|_{2^{2n-1}-1}$$

$$X = X^{(1)} + 2^n(2^{2n}-1)(2^{n-1}-1)P \tag{3.51}$$

where

$$P = ||(2^n(2^{2n}-1)(2^{n-1}-1))^{-1}|_{2^{2n-1}-1}(x_5 - X^{(1)})|_{2^{2n-1}-1} \tag{3.52}$$

Substituting the value of (3.49) in (3.42) we have

$$P = |(2^{2n-1} - 2^n - 2)(x_5 - X^{(1)})|_{2^{2n-1}-1} = |(-2^n - 1)(x_5 - X^{(1)})|_{2^{2n-1}-1}$$

$$= |(2^n + 1)(X^{(1)} - x_5)|_{2^{2n-1}-1} = |(2^n + 1)T|_{2^{2n-1}-1} \tag{3.53}$$

$$T = |a_1 + a_2 + a_3 + a_4|_{2^{2n-1}-1} \tag{3.54}$$

$$a_1 = \underbrace{Z_{n-2}Z_{n-3}\dots Z_1Z_0}_{n-1}\underbrace{x_{2,n-1}x_{2,n-2}\dots x_{2,1}x_{2,0}}_{n} \tag{3.55}$$

$$a_2 = \underbrace{Y_{n-2}Y_{n-3}\dots Y_1Y_0}_{n-1}\underbrace{0\dots00}_{n} \tag{3.56}$$

$$a_3 = \underbrace{0\dots00}_{n-2}\underbrace{Y_{2n-1}Y_{n-3}\dots Y_1Y_0}_{n+1} \tag{3.57}$$

$$a_4 = \underbrace{\overline{x_{5,2n-2}x_{5,2n-3}\dots x_{5,1}x_{5,0}}}_{2n-1} \tag{3.58}$$

Now, the value of P is simplified as:

$$P = |(2^n + 1)T|_{2^{2n-1}-1} = |a_5 + a_6|_{2^{2n-1}-1} \tag{3.59}$$

where

$$a_5 = \underbrace{T_{n-2}T_{n-3}\dots T_1T_0}_{n-1}\underbrace{T_{2n-2}T_{2n-3}\dots T_nT_{n-1}}_{n} \tag{3.60}$$

$$a_6 = \underbrace{T_{2n-2}T_{2n-3}\dots T_1T_0}_{2n-1} \tag{3.61}$$

The value of X in (3.51) can be simplified by substituting (3.50) as below:

$$X = x_2 + 2^nK + 2^n(2^{2n}-1)(2^{n-1}-1)P$$

$$= x_2 + 2^n(K + (2^{2n} - 1)(2^{n-1} - 1)P)$$

$$= x_2 + 2^n Q \tag{3.62}$$

Where

$$Q = K' + V \tag{3.63}$$

$$K' = \underbrace{0 \dots 00}_{2n-1}\ \underbrace{K_{3n-2}K_{3n-3} \dots K_1K_0}_{3n-1} \tag{3.64}$$

$$V = (2^{2n} - 1)(2^{n-1} - 1)P = (2^{3n-1} - 2^{2n} - 2^{n-1} + 1)P$$

$$V = a_7 + a_8\ (+1\ as\ carry\ in\ to\ CPA) \tag{3.65}$$

$$a_7 = \underbrace{P_{2n-2}P_{2n-3} \dots P_1P_0}_{2n-1}\ \underbrace{0 \dots 00}_{n}\ \underbrace{P_{2n-2}P_{2n-3} \dots P_1P_0}_{2n-1} \tag{3.66}$$

$$a_8 = \underbrace{1 \dots 11}_{n-1}\ \underbrace{\overline{a_{9,3n-1}a_{9,3n-2} \dots a_{9,1}a_{9,0}}}_{3n}\ \underbrace{1 \dots 11}_{n-1} \tag{3.67}$$

$$a_9 = a_{10} + a_{11} \tag{3.68}$$

$$a_{10} = \underbrace{P_{2n-2}P_{2n-3} \dots P_1P_0}_{2n-1}\ \underbrace{0 \dots 00}_{n+1} \tag{3.69}$$

$$a_{11} = \underbrace{P_{2n-2}P_{2n-3} \dots P_1P_0}_{2n-1}\ \underbrace{0 \dots 00}_{n+1} \tag{3.70}$$

Also, since x_2 is an n-bit number, *X* in (3.62) can be obtained as

$$X = x_2 + 2^n Q = \underbrace{Q_{5n-3}Q_{5n-4} \dots Q_1Q_0}_{5n-2}\ \underbrace{x_{2,n-1}x_{2,n-2} \dots x_{2,1}x_{2,0}}_{n} \tag{3.71}$$

Example: Consider the moduli set $\{2^n - 1, 2^n, 2^n + 1, 2^{n-1} - 1, 2^{2n-1} - 1\}$ where n=4. The weighted number *X* can be calculated from its RNS representation (7, 10, 3, 6, 18) as follows:

For n=4 the moduli set is {15, 16, 17, 7, 127} and also residues have binary representation as below

$$x_1 = 7 = (0111)_2$$

$$x_2 = 10 = (1010)_2$$

$$x_3 = 3 = (00011)_2$$

$$x_4 = 6 = (110)_2$$

$$x_5 = 18 = (0010010)_2$$

The values of Z, Y, K in (3.50) can be obtained from converter of [19] and their numerical values are given below:

$$Z = 1 = (001)_2$$

$$Y = 177 = (10110001)_2$$

$$K = 432 = (110110000)_2$$

According to (3.55), (3.56), (3.57), (3.58), (3.54), (3.60), (3.61), (3.69), (3.70), (3.68), (3.66), (3.67), (3.65), and (3.63) we have

$$a_1 = (0011010)_2 = 26$$

$$a_2 = (0010000)_2 = 16$$

$$a_3 = (0010110)_2 = 22$$

$$a_4 = (1101101)_2 = 109$$

$$T = |173|_{127} = (0101110)_2 = 46$$

$$a_5 = (1100101)_2 = 101$$

$$a_6 = (0101110)_2 = 46$$

$$P = |147|_{127} = 20 = (0010100)_2$$

$$a_{10} = (001010000000)_2 = 640$$

$$a_{11} = (000000010100)_2 = 20$$

$$a_9 = a_{10} + a_{11} = 660 = (001010010100)_2$$

$$a_7 = (0010100000000010100)_2 = 40980$$

$$a_8 = -(001010010100000)_2 = -5280$$

$$V = 40980 - 5280 = 35700$$

$$Q = K' + V = 432 + 35700 = 36132$$

Substituting the values of *Q* in (3.71), *X* can be calculated as:

$$X = (10001101001001001010)_2 = 578122$$

We can see that $|578122|_{15} = 7$, $|578122|_{16} = 10$, $|578122|_{17} = 3$, $|578122|_7 = 6$, $|578122|_{127} = 18$ and therefore the calculated *X* is indeed the weighted value of the residue representation (7, 10, 3, 6, 18) with respect to the moduli set {15, 16, 17, 7, 127}.

Hardware Implementation: The reverse converter hardware architecture for the five moduli set $\{2^n - 1, 2^n, 2^n + 1, 2^{n-1} - 1, 2^{2n-1} - 1\}$ with corresponding residues $(x_1, x_2, x_3, x_4, x_5)$ of the integer *X* is shown in Fig. 3.2. Area and Delay specification for each part of the converter are shown in Table 3.2.

3.1.3 Reverse Converter Design for $S_3 = \{2^{2n-1} - 1, 2^{2n} + 1, 2^n - 1, 2^n, 2^n + 1\}$:

Consider the five moduli set $S_3 = \{2^n, 2^{2n} + 1, 2^n + 1, 2^n - 1, 2^{2n-1} - 1\} = \{m_1, m_2, m_3, m_4, m_5\}$, where n is a natural number (n>1) and let the corresponding residues of the integer *X* be $(x_1, x_2, x_3, x_4, x_5)$. The residues have bit-level representations as:

$$x_1 = (x_{1,n-1}x_{1,n-2} \dots x_{1,1}x_{1,0})_2 \quad (3.72)$$

$$x_2 = (x_{2,2n}x_{2,2n-1} \dots x_{2,1}x_{2,0})_2 \quad (3.73)$$

$$x_3 = (x_{3,n}x_{3,n-1} \dots x_{3,1}x_{3,0})_2 \quad (3.74)$$

$$x_4 = (x_{4,n-1}x_{4,n-2} \dots x_{4,1}x_{4,0})_2 \quad (3.75)$$

$$x_5 = (x_{5,2n-2}x_{5,2n-3} \dots x_{5,1}x_{5,0})_2 \quad (3.76)$$

Table 3.2

Area and Delay Specification of Reverse Converter for the moduli set S_2 using New CRT I and MRC

Parts	**FA**	**NOT**	**XOR/AND pairs**	**XNOR/OR pairs**	**Delay**
OPU 1		2n-1			t_{NOT}
CSA1	1		2n-2		t_{FA}
CSA2	2n-1				t_{FA}
CPA1	2n-1				$(4n-2)t_{FA}$
OPU2	-				-
CPA2	2n-1				$(4n-2)t_{FA}$
OPU3	-				-
CPA3	n-2		2n+2		$3n\ t_{FA}$
OPU4		3n			t_{NOT}
CPA4	3n			2n-2	$(5n-2)t_{FA}$
OPU5	-				-
CPA5	3n-1		2n-1		$(5n-2)t_{FA}$
Area of Converter [19]		$0.5*(n^2+17n-6)A_{FA}+(5n+1)A_{NOT}+6A_{XOR}+6A_{AND}+(2n-8)A_{XNOR}+(2n-8)\ A_{OR}+2A_{MUX(1)}+A_{HA}$			
Delay of Converter [19]		$(11n+l-1)t_{FA}+2t_{NOT}+t_{MUX}$			
Total Area		$0.5*(n^2+43n-16)A_{FA}+(10n)A_{NOT}+(6n+5)A_{XOR}+(6n+5)A_{AND}+(4n-2)A_{XNOR}+(4n-2)\ A_{OR}+\ A_{HA}+2A_{MUX(1)}$			
Total Delay		$(32n-7+l)t_{FA}+4t_{NOT}+t_{MUX}$			

Here l is the minimum number of levels of CSA tree required to process (n/2) input operands.

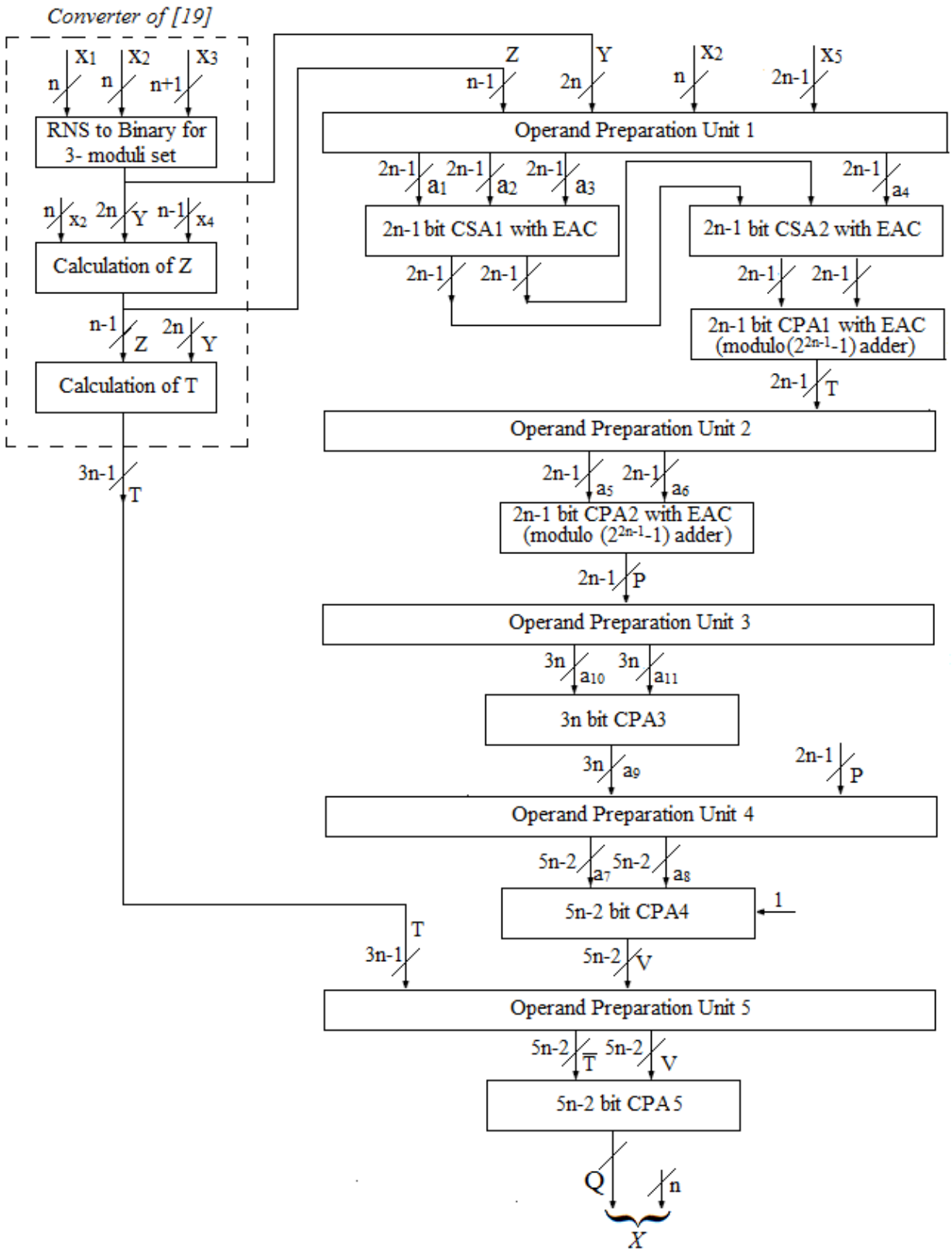


Figure 3.2 Reverse Converter for the moduli set S_2 using New CRT I and MRC

The following sections describe the design of reverse converter for S_3 using New CRT I and MRC conversion algorithms in two different methods.

3.1.3.1 Reverse Converter Design for S_3 Using New CRT I and MRC (Method 1):

The set S_3 here is decomposed into two subsets $A_1 = \{2^n, 2^{2n}+1, 2^n+1, 2^n-1\}$ and $A_2 = \{2^{2n-1}-1\}$. An integer $X^{(1)}$ is calculated from the residues x_1, x_2, x_3, x_4 of A_1. The conversion algorithm New CRT I is used to calculate $X^{(1)}$. Next, the MRC algorithm is applied to calculate the integer X from the residues $(X^{(1)}, x_5)$ corresponding to the moduli set $A_3 = \{2^n(2^{4n}-1), 2^{2n-1}-1\}$. The following propositions are needed for the derivation of X.

Proposition 1: The multiplicative inverse of 2^n modulo $2^{4n}-1$ is:

$$|m_1^{-1}|_{m_2 m_3 m_4} = |(2^n)^{-1}|_{2^{4n}-1} = 2^{3n} \tag{3.77}$$

where n is natural number larger than 1.

Proof: Using property of equation (1.35), if $|a^{-1}|_m = b$ then $|a \cdot b|_m = 1$

Since $|(2^n)^{-1}|_{2^{4n}-1} = 2^{3n}$, we have

$$|2^n \cdot 2^{3n}|_{2^{4n}-1} = |2^{4n}|_{2^{4n}-1} = 1$$

Proposition 2: The multiplicative inverse of $2^n(2^{2n}+1)$ modulo $2^{2n}-1$ is:

$$|(m_1 m_2)^{-1}|_{m_3 m_4} = |(2^n \cdot 2^{2n}+1)^{-1}|_{2^{2n}-1} = 2^{n-1} \tag{3.78}$$

where n is natural number larger than 1.

Proof: Using property of equation (1.35), if $|a^{-1}|_m = b$ then $|a \cdot b|_m = 1$

Since $|(2^n(2^{2n}+1))^{-1}|_{2^{2n}-1} = 2^{n-1}$, we have

$$|2^n(2^{2n}+1)2^{n-1}|_{2^{2n}-1} = |2^{2n-1}(2^{2n}+1)|_{2^{2n}-1} = |2^{2n-1}(2)|_{2^{2n}-1} = |2^{2n}|_{2^{2n}-1} = 1$$

Proposition 3: The multiplicative inverse of $2^n(2^{2n}+1)(2^n+1)$ modulo 2^n-1 is:

$$|(m_1 m_2 m_3)^{-1}|_{m_4} = |(2^n(2^{2n}+1)(2^n+1))^{-1}|_{2^n-1} = 2^{n-2} \tag{3.79}$$

where n is natural number larger than 1.

Proof: Using property of equation (1.35), if $|a^{-1}|_m = b$ then $|a \cdot b|_m = 1$

Since $|(2^n(2^{2n}+1)(2^n+1))^{-1}|_{2^n-1} = 2^{n-2}$, we have

$$|2^n(2^{2n}+1)(2^n+1)2^{n-2}|_{2^n-1} = |1 \cdot 2 \cdot 2 \cdot 2^{n-2}|_{2^n-1} = |2^n|_{2^n-1} = 1$$

Proposition 4: The multiplicative inverse of $2^n(2^{4n}-1)$ modulo $2^{2n-1}-1$ is:

$$|(2^n(2^{4n}-1))^{-1}|_{2^{2n-1}-1} = \begin{cases} \sum_{l=0}^{n-2} 2^l + \sum_{m=n-1}^{2n-3} 2^m & if\ n = 2k, k = 1,2,3 \ldots \\ \sum_{l=n-1}^{2n-2} 2^l + \sum_{m=1}^{n-2} 2^m & if\ n = 2k+1, k = 1,2,3 \ldots \end{cases} \quad (3.80)$$

where n is natural number(n>1), l is even, m is odd. The above expression contains n terms.

Examples: The following values of multiplicative inverse for different values of n are found using the program given in Appendix A (Section A.2).

The value of $|(2^n(2^{4n}-1))^{-1}|_{2^{2n-1}-1}$ for different values of n is:

For $n = 2$, $|(2^n(2^{4n}-1))^{-1}|_{2^{2n-1}-1} = |1020^{-1}|_7$=3

$= (11)_2\ in\ binary$

$= 2^0 + 2^1$

For $n = 3$, $|(2^n(2^{4n}-1))^{-1}|_{2^{2n-1}-1} = |32760^{-1}|_{31}$=22

$= (10110)_2$

$= 2^1 + 2^2 + 2^4$

For $n = 4$, $|(2^n(2^{4n}-1))^{-1}|_{2^{2n-1}-1} = |1048560^{-1}|_{127}$=45

$= (101101)_2$

$= 2^0 + 2^2 + 2^3 + 2^5$

For $n = 5$, $|(2^n(2^{4n}-1))^{-1}|_{2^{2n-1}-1} = |33554400^{-1}|_{511}$=346

$= (101011010)_2$

$$= 2^1 + 2^3 + 2^4 + 2^6 + 2^8$$

Thus the above values of $|(2^n(2^{4n}-1))^{-1}|_{2^{2n-1}-1}$ can be generalized as follows,

$$|(2^n(2^{4n}-1))^{-1}|_{2^{2n-1}-1} = \begin{cases} \sum_{l=0}^{n-2} 2^l + \sum_{m=n-1}^{2n-3} 2^m & if\ n = 2k, k = 1,2,3 \dots \\ \sum_{l=n-1}^{2n-2} 2^l + \sum_{m=1}^{n-2} 2^m & if\ n = 2k+1, k = 1,2,3 \dots \end{cases}$$

where n is natural number(n>1), *l* is even, m is odd.

Calculation of $X^{(1)}$*:*

The value of $X^{(1)}$ is calculated from New CRT I as follows:

$$X^{(1)} = x_1 + m_1|\, k_1(x_2 - x_1) + k_2 m_2(x_3 - x_2) + k_3 m_2 m_3(x_4 - x_3)|_{m_2 m_3 m_4} \quad (3.81)$$

where

$$k_1 = |m_1^{-1}|_{m_2 m_3 m_4},\ k_2 = |(m_1 m_2)^{-1}|_{m_3 m_4} \text{ and } k_3 = |(m_1 m_2 m_3)^{-1}|_{m_4} \quad (3.82)$$

Substituting the values of (3.77), (3.78), (3.79), m_1, m_2 and m_3 in (3.81) we have

$$X^{(1)} = x_1 + 2^n|2^{3n}(x_2 - x_1) + 2^{n-1}(2^{2n}+1)(x_3 - x_2) + 2^{n-2}(2^n+1)(2^{2n}+1)(x_4 - x_3)\,|_{2^{4n}-1}$$

$$= x_1 + 2^n M \quad (3.83)$$

where

$$M = |\, a_1 + a_2 + a_3 + a_4 + a_5\,|_{2^{4n}-1} \quad (3.84)$$

$$a_1 = \underbrace{x_{2,n}x_{2,n-1}\dots x_{2,1}x_{2,0}}_{n+1}\ \underbrace{0\dots00}_{2n-1}\ \underbrace{x_{2,2n}x_{2,2n-1}\dots x_{2,n+2}x_{2,n+1}}_{n} \quad (3.85)$$

$$a_2 = \underbrace{x_{4,1}x_{4,0}}_{2}\ \underbrace{x_{4,n-1}\dots x_{4,1}x_{4,0}}_{n}\ \underbrace{x_{4,n-1}\dots x_{4,1}x_{4,0}}_{n}\ \underbrace{x_{4,n-1}\dots x_{4,1}x_{4,0}}_{n}\ \underbrace{x_{4,n-1}\dots x_{4,3}x_{4,2}}_{n-2} \quad (3.86)$$

$$a_3 = \underbrace{\overline{x_{1,n-1}x_{1,n-2}\dots x_{1,1}x_{1,0}}}_{n}\ \underbrace{1}_{1}\ \underbrace{\overline{x_{3,n}x_{3,n-1}\dots x_{3,1}x_{3,0}}}_{n+1}\ \underbrace{1\dots11}_{2n-2} \quad (3.87)$$

$$a_4 = \underbrace{0}_{1}\ \underbrace{x_{3,n}x_{3,n-1}\dots x_{3,1}x_{3,0}}_{n+1}\ \underbrace{0\dots00}_{n-1}\ \underbrace{x_{3,n}x_{3,n-1}\dots x_{3,1}x_{3,0}}_{n+1}\ \underbrace{0\dots00}_{n-2} \quad (3.88)$$

$$a_5 = \underbrace{\overline{x_{3,1}x_{3,0}}}_{2}\ \underbrace{1\ldots11}_{n-2}\ \underbrace{\overline{x_{2,n}x_{2,n-1}\ldots x_{2,1}x_{2,0}}}_{2n+1}\ \underbrace{\overline{x_{3,n}x_{3,n-1}\ldots x_{3,3}x_{3,2}}}_{n-1} \tag{3.89}$$

Calculation of X:

The value of *X* is calculated from MRC as follows:

$$\begin{aligned} X &= X^{(1)} + 2^n(2^{4n}-1)||(2^n(2^{4n}-1))^{-1}|_{2^{2n-1}-1} \cdot \left(x_5 - X^{(1)}\right)|_{2^{2n-1}-1} \\ &= X^{(1)} + 2^n(2^{4n}-1)P \end{aligned} \tag{3.90}$$

where

$$P = ||(2^n(2^{2n}-1))^{-1}|_{2^{2n-1}-1}T|_{2^{2n-1}-1} \text{ and } T = |\left(x_5 - X^{(1)}\right)|_{2^{2n-1}-1} \tag{3.91}$$

$$T = |x_5 - x_1 - 2^nM|_{2^{2n-1}-1} = |a_6 + a_7 + a_8 + a_9|_{2^{2n-1}-1} \tag{3.92}$$

$$a_6 = \underbrace{x_{5,2n-2}x_{5,2n-3}\ldots x_{5,1}x_{5,0}}_{2n-1} \tag{3.93}$$

$$a_7 = \underbrace{1\ldots11}_{n-3}\ \underbrace{\overline{M_{4n-1}M_{4n-2}\ldots M_{3n-1}M_{3n-2}}}_{n+2} \tag{3.94}$$

$$a_8 = \underbrace{\overline{M_{3n-3}M_{3n-2}\ldots M_nM_{n-1}}}_{2n-1} \tag{3.95}$$

$$a_9 = \underbrace{\overline{M_{n-2}M_{n-3}\ldots M_1M_0}}_{n-1}\ \underbrace{\overline{x_{5,2n-2}x_{5,2n-3}\ldots x_{5,1}x_{5,0}}}_{n} \tag{3.96}$$

The value of *P* in equation (3.91) can be simplified by substituting value of equation (3.80) and operating circular left shift on bits of *T*.

The value of *X* in the equation (3.91) can be simplified by substituting equation (3.83) as:

$$\begin{aligned} X &= X^{(1)} + 2^n(2^{4n}-1)P \ = x_1 + 2^nM + 2^n(2^{4n}-1)P \\ &= x_1 + 2^n(M + (2^{4n}-1)P) \\ &= x_1 + 2^nQ \end{aligned} \tag{3.97}$$

where

$$Q = M + (2^{4n}-1)P = M + 2^{4n}P - P = K - P \tag{3.98}$$

$$K = M + 2^{4n}P = \underbrace{P_{2n-2}P_{2n-2}\dots P_1P_0}_{2n-1}\underbrace{M_{4n-1}M_{4n-2}\dots M_1M_0}_{4n} \quad (3.99)$$

Also, since x_1 is an n-bit number, *X* in (3.97) can be obtained as

$$X = x_1 + 2^nQ = \underbrace{Q_{6n-2}Q_{6n-3}\dots Q_1Q_0}_{6n-1}\underbrace{x_{1,n-1}x_{1,n-2}\dots x_{1,1}x_{1,0}}_{n} \quad (3.100)$$

Example: Consider the moduli set $\{2^n, 2^{2n}+1, 2^n+1, 2^n-1, 2^{2n-1}-1\}$ where n=4. The weighted number *X* can be calculated from its RNS representation (9, 223, 15, 1, 13) as follows:

For n=4 the moduli set is {16, 257, 17, 15, 127} and also residues have binary representation as below

$$x_1 = 9 = (1001)_2$$

$$x_2 = 223 = (011011111)_2$$

$$x_3 = 15 = (01111)_2$$

$$x_4 = 1 = (0001)_2$$

$$x_5 = 13 = (0001101)_2$$

According to (3.84), (3.93), (3.94), (3.95), (3.96), (3.92), and (3.91) we have

$$M = |204232|_{65535} = (0001110111001011)_2 = 7627$$

$$a_6 = (0001101)_2 = 13$$

$$a_7 = (1111000)_2 = 120$$

$$a_8 = (1000110)_2 = 70$$

$$a_9 = (1000110)_2 = 70$$

$$T = |273|_{127} = 19 = (0010011)_2$$

$$P = |855|_{127} = 93 = (1011101)_2$$

Substituting the values of *M* and *P* in *Q*, *X* can be calculated from (3.99), (3.98) and (3.100) as below

$$K = (10111010001110111001011)_2 = 6102475$$

$$Q = 6102475 - 93 = 6102382$$

$$X = (101110100011101011011101001)_2 = 97638121$$

We can see that $|97638121|_{16} = 9$, $|97638121|_{257} = 223$, $|97638121|_{17} = 15$, $|97638121|_{15} = 1$, $|97638121|_{127} = 13$ and therefore the calculated *X* is indeed the weighted value of the residue representation (9, 223, 15, 1, 13) with respect to the moduli set {16, 257, 17, 15, 127}.

Hardware Implementation: The reverse converter hardware architecture for the five moduli set $\{2^n, 2^{2n}+1, 2^n+1, 2^n-1, 2^{2n-1}-1\}$ with corresponding residues $(x_1, x_2, x_3, x_4, x_5)$ of the integer *X* is shown in Fig. 3.3. Area and Delay specification for each part of the converter are shown in Table 3.3.

3.1.3.2 Reverse Converter Design for S_3 Using New CRT I and MRC (Method 2):

The set S_3 here is decomposed into two subsets $A_1 = \{2^n, 2^{2n-1}-1\}$ and $A_2 = \{2^{2n}+1, 2^n-1, 2^n+1\}$. Two interim integers $X^{(1)}$ and $X^{(2)}$ are calculated from the residues x_1, x_2 of A_1 and x_3, x_4, x_5 of A_2. The conversion algorithms MRC and New CRT I are used to calculate $X^{(1)}$ and $X^{(2)}$ respectively. Next, the MRC algorithm is applied to calculate the integer *X* from the residues $(X^{(1)}, X^{(2)})$ corresponding to the moduli set $A_3 = \{2^n(2^{2n-1}-1), 2^{4n}-1\}$. The following propositions are needed for the derivation of *X*.

Proposition 1: The multiplicative inverse of 2^n modulo $2^{2n-1}-1$ is:

Table 3.3

Area and Delay Specification of Reverse Converter for the moduli set S_3 using New CRT I and MRC (Method 1)

Parts	**FA**	**NOT**	**XOR/AND pairs**	**XNOR/OR pairs**	**Delay**
OPU 1		5n+3			t_{NOT}
CSA1	n+3		2n-1	n-2	t_{FA}
CSA2	2n+1			2n-1	t_{FA}
CSA3	2n+2		2n-2		t_{FA}
CPA1	4n				$8n\ t_{FA}$
OPU2		5n			t_{NOT}
CSA4	n+2			n-3	t_{FA}
CSA5	2n-1				t_{FA}
CPA2	2n-1				$(4n-2)t_{FA}$
OPU3	-				-
CSA6 Tree	$2n^2$-5n+2				$l \cdot t_{FA}$
CPA3	2n-1				$(4n-2)t_{FA}$
OPU4		2n-1			t_{NOT}
CPA4	2n-1			4n	$(6n-1)t_{FA}$
Total Area		$(2n^2+13n+6)A_{FA}$+ (12n+2)A_{NOT}+ (4n-3)A_{XOR}+ (4n-3)A_{AND}+ (8n-6)A_{XNOR}+ (8n-6) A_{OR}			
Total Delay		$(22n+l)t_{FA}$ + $3t_{NOT}$			

Here *l* is the minimum number of levels of CSA tree required to process (n) input operands.

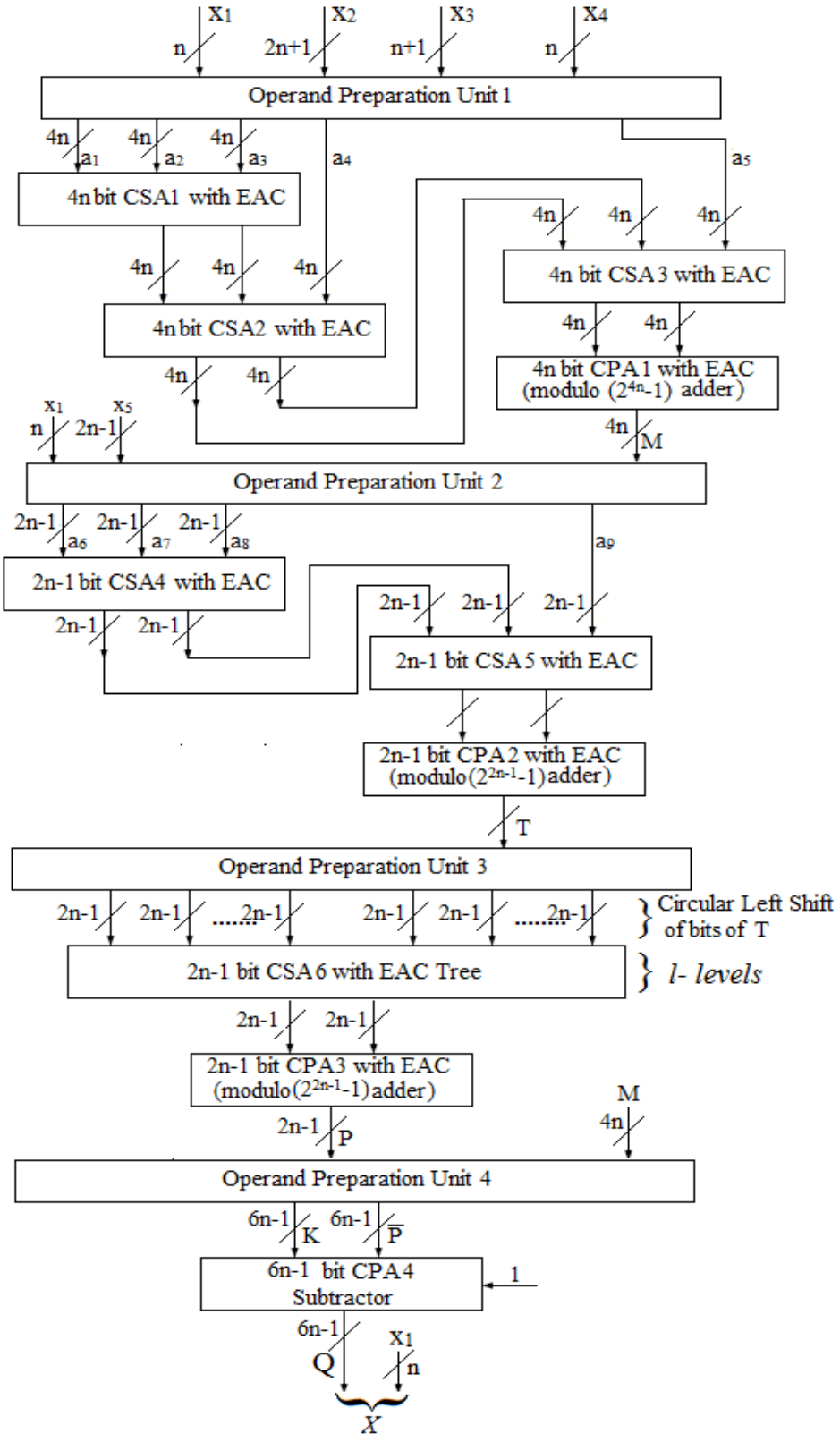


Figure 3.3. Reverse Converter for the moduli set S_3 using New CRT I and MRC (Method 1)

$$|m_1^{-1}|_{m_2} = |(2^n)^{-1}|_{2^{2n-1}-1} = 2^{n-1} \tag{3.101}$$

where n is natural number larger than 1.

Proof: Using property of equation (1.35), if $|a^{-1}|_m = b$ then $|a \cdot b|_m = 1$

Since $|(2^n)^{-1}|_{2^{2n-1}-1} = 2^{n-1}$, we have

$$|2^n \cdot 2^{n-1}|_{2^{2n-1}-1} = |2^{2n-1}|_{2^{2n-1}-1} = 1$$

Proposition 2: The multiplicative inverse of $(2^{2n}+1)$ modulo $2^{2n}-1$ is:

$$|(m_3)^{-1}|_{m_4 m_5} = |(2^{2n}+1)^{-1}|_{2^{2n}-1} = 2^{2n-1} \tag{3.102}$$

where n is natural number larger than 1.

Proof: Using property of equation (1.35), if $|a^{-1}|_m = b$ then $|a \cdot b|_m = 1$

Since $|(2^{2n}+1)^{-1}|_{2^{2n}-1} = 2^{2n-1}$, we have

$$|(2^{2n}+1)2^{2n-1}|_{2^{2n}-1} = |2 \cdot 2^{2n-1})|_{2^{2n}-1} = |2^{2n}|_{2^{2n}-1} = 1$$

Proposition 3: The multiplicative inverse of $(2^n-1)(2^{2n}+1)$ modulo 2^n+1 is:

$$|(m_3 m_4)^{-1}|_{m_5} = |((2^n-1)(2^{2n}+1))^{-1}|_{2^n+1} = 2^{n-2} \tag{3.103}$$

where n is natural number larger than 1.

Proof: Using property of equation (1.35), if $|a^{-1}|_m = b$ then $|a \cdot b|_m = 1$

Since $|((2^n-1)(2^{2n}+1))^{-1}|_{2^n+1} = 2^{n-2}$, we have

$$|(2^n-1)(2^{2n}+1)2^{n-2}|_{2^n+1} = |-2 \cdot 2 \cdot 2^{n-2}|_{2^n+1} = |-2^n|_{2^n+1} = |2^n+1-2^n|_{2^n+1} = 1$$

Proposition 4: The multiplicative inverse of $2^n(2^{2n-1}-1)$ modulo $2^{4n}-1$ is:

$$|(2^n(2^{2n-1}-1))^{-1}|_{2^{4n}-1} = \begin{cases} \sum_{l=1}^{n-1} 2^l + \sum_{m=n+2}^{3n} 2^m + \sum_{i=3n+3}^{4n-1} 2^i & if\ n = 2k, k = 1,2,3 \dots \\ \sum_{l=n+2}^{3n} 2^l + \sum_{m=0}^{n-1} 2^m + \sum_{j=3n+3}^{4n-2} 2^j & if\ n = 2k+1, k = 1,2,3 \dots \end{cases} \tag{3.104}$$

where n is natural number(n>1), *l* is odd, *m* is even, *i* is odd, *j* is even. The above expression contains $(2n-1)$ terms.

Examples: The following values of multiplicative inverse for different values of n are found using the program given in Appendix A (Section A.2).

The value of $|(2^n(2^{2n-1}-1))^{-1}|_{2^{4n}-1}$ for different values of n is:

For $n=2, |(2^n(2^{2n-1}-1))^{-1}|_{2^{4n}-1} = |28^{-1}|_{255}$=82

$$= (1010010)_2 \; in \; binary$$

$$= 2^1 + 2^4 + 2^6$$

For $n=3, |(2^n(2^{2n-1}-1))^{-1}|_{2^{4n}-1} = |248^{-1}|_{4095}$=677

$$= (1010100101)_2$$

$$= 2^0 + 2^2 + 2^5 + 2^7 + 2^9$$

For $n=4, |(2^n(2^{2n-1}-1))^{-1}|_{2^{4n}-1} = |2032^{-1}|_{65535}$=38218

$$= (1001010101001010)_2$$

$$= 2^1 + 2^3 + 2^6 + 2^8 + 2^{10} + 2^{12} + 2^{15}$$

For $n=5, |(2^n(2^{2n-1}-1))^{-1}|_{2^{4n}-1} = |16352^{-1}|_{1048575}$=305813

$$= (1001010101010010101)_2$$

$$= 2^0 + 2^2 + 2^4 + 2^7 + 2^9 + 2^{11} + 2^{13} + 2^{15} + 2^{18}$$

Thus the above values of $|(2^n(2^{2n-1}-1))^{-1}|_{2^{4n}-1}$ can be generalized as follows,

$$|(2^n(2^{2n-1}-1))^{-1}|_{2^{4n}-1} = \begin{cases} \sum_{l=1}^{n-1} 2^l + \sum_{m=n+2}^{3n} 2^m + \sum_{i=3n+3}^{4n-1} 2^i & if\ n = 2k, k = 1,2,3 \dots \\ \sum_{l=n+2}^{3n} 2^l + \sum_{m=0}^{n-1} 2^m + \sum_{j=3n+3}^{4n-2} 2^j & if\ n = 2k+1, k = 1,2,3 \dots \end{cases}$$

where n is natural number(n>1), *l* is odd, m is even, i is odd, j is even.

Calculation of $X^{(1)}$:

The value of $X^{(1)}$ is calculated from MRC as follows:

$$X^{(1)} = x_1 + m_1 \cdot | \, |m_1^{-1}|_{m_2} \cdot (x_2 - x_1) \, |_{m_2} \tag{3.105}$$

Substituting the value (3.101), m_1 and m_2 in (3.105) we have

$$X^{(1)} = x_1 + 2^n \cdot | \, 2^{n-1} \cdot (x_2 - x_1) \, |_{2^{2n-1}-1}$$

$$= x_1 + 2^n M \tag{3.106}$$

where

$$M = |a_1 + a_2|_{2^{2n-1}-1} \tag{3.107}$$

$$a_1 = \underbrace{x_{2,n-1}x_{2,n-2} \dots x_{2,0}}_{n} \underbrace{x_{2,2n-2}x_{2,2n-3} \dots x_{2,n}}_{n-1} \tag{3.108}$$

$$a_2 = \underbrace{\overline{x_{1,n-1} \dots x_{1,0}}}_{n} \underbrace{1 \dots 11}_{n-1} \tag{3.109}$$

Calculation of $X^{(2)}$:

The value of $X^{(2)}$ is calculated from New CRT I as follows:

$$X^{(2)} = x_3 + m_3 | \, |m_3^{-1}|_{m_4 m_5}(x_4 - x_3) + |(m_3 m_4)^{-1}|_{m_5} m_4 (x_5 - x_4)|_{m_4 m_5} \tag{3.110}$$

Substituting the values of (3.102), (3.103), m_3, m_4 and m_5 in (3.110) we have

$$X^{(2)} = x_3 + (2^{2n} + 1)|2^{2n-1}(x_4 - x_3) + 2^{n-2}(2^n - 1)(x_5 - x_4)|_{2^{2n}-1}$$

$$= x_3 + (2^{2n} + 1)N \tag{3.111}$$

where

$$N = | \, a_3 + a_4 + a_5 + a_6 \, |_{2^{2n}-1} \tag{3.112}$$

$$a_3 = \underbrace{x_{4,1}x_{4,0}}_{2} \underbrace{x_{4,n-1} \dots x_{4,1}x_{4,0}}_{n} \underbrace{x_{4,n-1} \dots x_{4,3}x_{4,2}}_{n-2} \tag{3.113}$$

$$a_4 = \begin{cases} a_{41} = \underbrace{0}_{1} \underbrace{1 \dots 11}_{2n-1} & if \;\; x_{3,2n} = 1 \\ a_{42} = \underbrace{\overline{x_{3,0}x_{3,2n-1} \dots x_{3,2}x_{3,1}}}_{2n} & if \;\; x_{3,2n} = 0 \end{cases} \tag{3.114}$$

$$a_5 = \underbrace{x_{5,1}x_{5,0}}_{2}\,\underbrace{0\ldots00}_{n-1}\,\underbrace{x_{5,n}\ldots x_{5,3}x_{5,2}}_{n-1} \tag{3.115}$$

$$a_6 = \underbrace{1}_{1}\,\underbrace{\overline{x_{5,n}x_{5,n-1}\ldots x_{5,1}x_{5,0}}}_{n+1}\,\underbrace{1\ldots11}_{n-2} \tag{3.116}$$

Calculation of X:

The value of *X* is calculated from MRC as follows:

$$\begin{aligned} X &= X^{(1)} + 2^n(2^{2n-1}-1)\,||(2^n(2^{2n-1}-1))^{-1}|_{2^{4n}-1} \cdot \left(X^{(2)} - X^{(1)}\right)|_{2^{4n}-1} \\ &= X^{(1)} + 2^n(2^{2n-1}-1)P \end{aligned} \tag{3.117}$$

where

$$P = ||(2^n(2^{2n-1}-1))^{-1}|_{2^{4n}-1}T|_{2^{4n}-1} \text{ and } T = |\left(X^{(2)} - X^{(1)}\right)|_{2^{4n}-1} \tag{3.118}$$

$$T = |x_3 + (2^{2n}+1)N - x_1 - 2^nM|_{2^{4n}-1} = |a_7 + a_8 + a_9|_{2^{4n}-1} \tag{3.119}$$

$$a_7 = \underbrace{0\ldots00}_{2n-1}\,\underbrace{x_{3,2n}x_{3,2n-1}\ldots x_{3,1}x_{3,0}}_{2n+1} \tag{3.120}$$

$$a_8 = \underbrace{N_{2n-1}N_{2n-2}\ldots N_1N_0}_{2n}\,\underbrace{N_{2n-1}N_{2n-2}\ldots N_1N_0}_{2n} \tag{3.121}$$

$$a_9 = \underbrace{1\ldots11}_{n+1}\,\underbrace{\overline{M_{2n-2}M_{2n-3}\ldots M_1M_0}}_{2n-1}\,\underbrace{\overline{x_{1,n-1}x_{1,n-2}\ldots x_{1,1}x_{1,0}}}_{n} \tag{3.122}$$

The value of *P* in equation (3.118) can be simplified by substituting value of equation (3.104) and operating circular left shift on bits of *T*.

The value of *X* in the equation (3.117) can be simplified by substituting equation (3.106) as:

$$\begin{aligned} X &= X^{(1)} + 2^n(2^{2n-1}-1)P \;\; = x_1 + 2^nM + 2^n(2^{2n-1}-1)P \\ &= x_1 + 2^n(M + (2^{2n-1}-1)P) \\ &= x_1 + 2^nQ \end{aligned} \tag{3.123}$$

where

$$Q = M + (2^{2n-1}-1)P = M + 2^{2n-1}P - P = K - P \tag{3.124}$$

$$K = M + 2^{2n-1}P = \underbrace{P_{4n-1}P_{4n-2}\dots P_1P_0}_{4n}\,\underbrace{M_{2n-2}M_{2n-3}\dots M_1M_0}_{2n-1} \qquad (3.125)$$

Also, since x_1 is an n-bit number, *X* in (3.123) can be obtained as

$$X = x_1 + 2^nQ = \underbrace{Q_{6n-2}Q_{6n-3}\dots Q_1Q_0}_{6n-1}\,\underbrace{x_{1,n-1}x_{1,n-2}\dots x_{1,1}x_{1,0}}_{n} \qquad (3.126)$$

Example: Consider the moduli set $\{2^n, 2^{2n-1}-1, 2^{2n}+1, 2^n-1, 2^n+1\}$ where n=3. The weighted number *X* can be calculated from its RNS representation (0, 5, 26, 0, 2) as follows:

For n=3 the moduli set is {8, 31, 65, 7, 9} and also residues have binary representation as below

$$x_1 = 0 = (000)_2$$

$$x_2 = 5 = (00101)_2$$

$$x_3 = 26 = (0011010)_2$$

$$x_4 = 0 = (000)_2$$

$$x_5 = 2 = (0010)_2$$

According to (3.108), (3.109), (3.107), (3.113), (3.114), (3.115), (3.116), (3.112), (3.120), (3.121), (3.122), (3.119), and (3.118) we have

$$a_1 = (10100)_2 = 20$$

$$a_2 = (11111)_2 = 31$$

$$M = |51|_{31} = (10100)_2 = 20$$

$$a_3 = (000000)_2 = 0$$

$$a_4 = (110010)_2 = 50$$

$$a_5 = (100000)_2 = 32$$

$$a_6 = (111011)_2 = 59$$

$$N = |141|_{63} = 15 = (001111)_2$$

$$a_7 = (000000011010)_2 = 26$$

$$a_8 = (001111001111)_2 = 975$$

$$a_9 = (111101011111)_2 = 3935$$

$$T = |4936|_{4095} = 841 = (001101001001)_2$$

$$P = |569357|_{4095} = 152 = (000010011000)_2$$

Substituting the values of *M* and *P* in *Q*, *X* can be calculated from (3.125), (3.124) and (3.126) as below

$$K = (00001001100010100)_2 = 4884$$

$$Q = 4884 - 152 = 4732$$

$$X = (1001001111100000)_2 = 97638121$$

We can see that $|37856|_8 = 0$, $|37856|_{31} = 5$, $|37856|_{65} = 26$, $|37856|_7 = 0$, $|37856|_9 = 2$ and therefore the calculated *X* is indeed the weighted value of the residue representation (0, 5, 26, 0, 2) with respect to the moduli set {8, 31, 65, 7, 9}.

Hardware Implementation: The reverse converter hardware architecture for the five moduli set $\{2^n, 2^{2n}+1, 2^n+1, 2^n-1, 2^{2n-1}-1\}$ with corresponding residues $(x_1, x_2, x_3, x_4, x_5)$ of the integer *X* is shown in Fig. 3.4. Area and Delay specification for each part of the converter are shown in Table 3.4.

3.1.4 Reverse Converter Design for $S_4 = \{2^{2n-1}-1, 2^{2n}+1, 2^n-1, 2^{2n}, 2^n+1\}$:

Consider the five moduli set $S_4 = \{2^{2n}, 2^{2n}+1, 2^n+1, 2^n-1, 2^{2n-1}-1\} = \{m_1, m_2, m_3, m_4, m_5\}$, where n is a natural number (n>1) and let the corresponding residues of the integer *X* be $(x_1, x_2, x_3, x_4, x_5)$. The residues have bit-level representations as:

Table 3.4

Area and Delay Specification of Reverse Converter for the moduli set S_3 using New CRT I and MRC (Method 2)

Parts	**FA**	**NOT**	**XOR/AND pairs**	**XNOR/OR pairs**	**MUX**	**Delay**
OPU 1		4n+1			1 (2n) bit	$t_{NOT} + t_{MUX}$
CPA1	n			n-1		$(4n-2)t_{FA}$
CSA1	n+1		n-1			t_{FA}
CSA2	n+1			n-1		t_{FA}
CPA2	2n					$4n\ t_{FA}$
OPU2		3n-1				t_{NOT}
CSA3	2n+1		2n-1			t_{FA}
CPA3	4n					$8n\ t_{FA}$
OPU3	-					-
CSA4 Tree	$8n^2$-12n					$l \cdot t_{FA}$
CPA4	4n					$8n\ t_{FA}$
OPU4		4n				t_{NOT}
CPA5	4n			2n-1		$(6n-1)t_{FA}$
Total Area		$(8n^2+9n+3)A_{FA}$+ (11n)A_{NOT}+ (3n-2)A_{XOR}+ (3n-2)A_{AND}+ (4n-3)A_{XNOR}+ (4n-3)A_{OR} + $A_{MUX(2n)}$				
Total Delay		$(26n+2+l)t_{FA}$ + $3t_{NOT}$ + t_{MUX}				

Here *l* is the minimum number of levels of CSA tree required to process (2n-1) input operands.

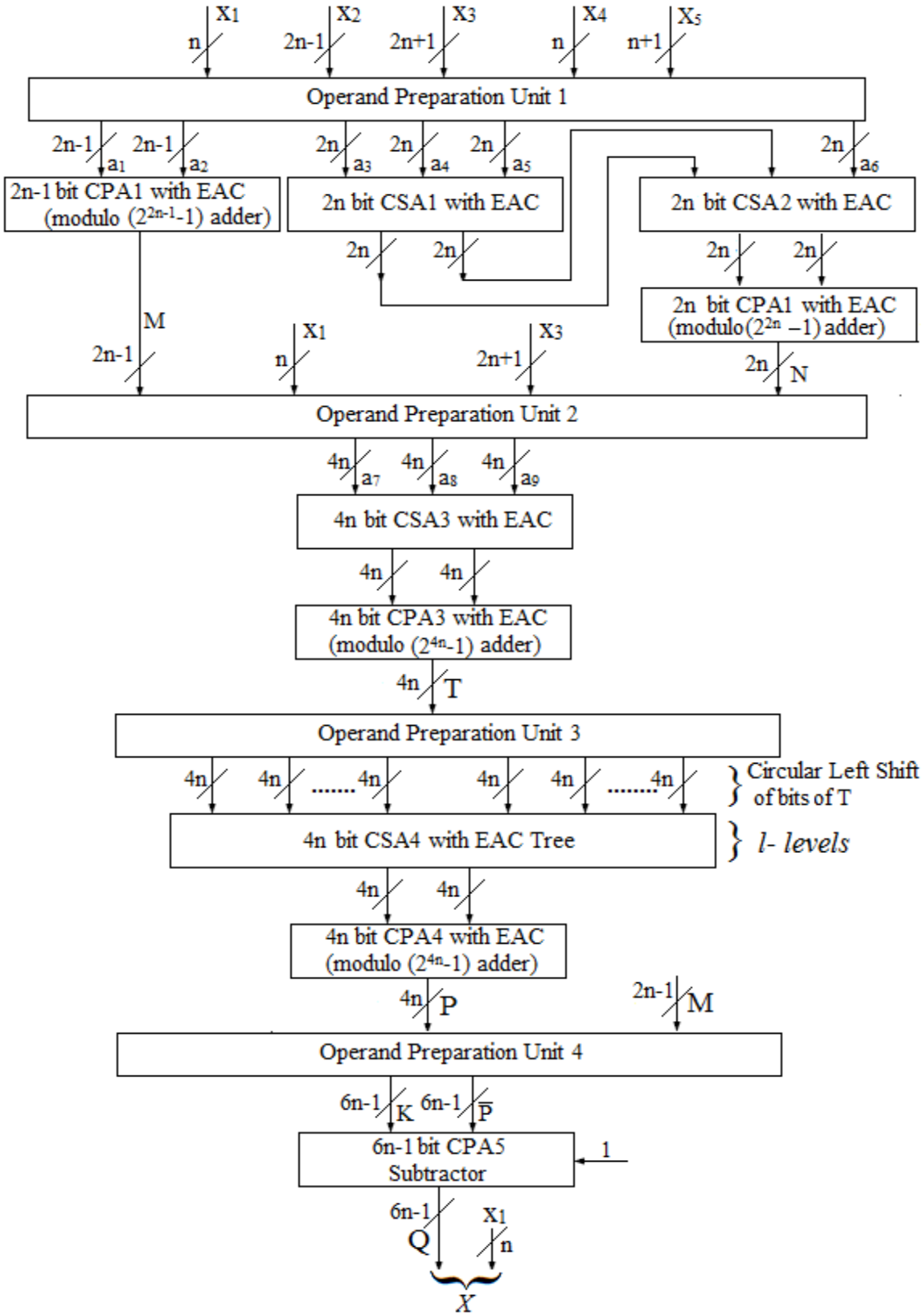


Figure 3.4 Reverse Converter for the moduli set S_3 using New CRT I and MRC (Method 2)

$$x_1 = (x_{1,2n-1}x_{1,2n-2} \dots x_{1,1}x_{1,0})_2 \quad (3.127)$$

$$x_2 = (x_{2,2n}x_{2,2n-1} \dots x_{2,1}x_{2,0})_2 \quad (3.128)$$

$$x_3 = (x_{3,n}x_{3,n-1} \dots x_{3,1}x_{3,0})_2 \quad (3.129)$$

$$x_4 = (x_{4,n-1}x_{4,n-2} \dots x_{4,1}x_{4,0})_2 \quad (3.130)$$

$$x_5 = (x_{5,2n-2}x_{5,2n-3} \dots x_{5,1}x_{5,0})_2 \quad (3.131)$$

The following sections describe the design of reverse converter for S_4 using New CRT I and MRC conversion algorithms in two different methods.

3.1.4.1 Reverse Converter Design for S_4 Using New CRT I and MRC (Method 1):

The set S_3 here is decomposed into two subsets $A_1 = \{2^{2n}, 2^{2n}+1, 2^n+1, 2^n-1\}$ and $A_2 = \{2^{2n-1}-1\}$. An integer $X^{(1)}$ is calculated from the residues x_1, x_2, x_3, x_4 of A_1. The conversion algorithm New CRT I is used to calculate $X^{(1)}$. Next, the MRC algorithm is applied to calculate the integer X from the residues $(X^{(1)}, x_5)$ corresponding to the moduli set $A_3 = \{2^{2n}(2^{4n}-1), 2^{2n-1}-1\}$. The following proposition is needed for the derivation of X.

Proposition 1: The multiplicative inverse of $2^{2n}(2^{4n}-1)$ modulo $2^{2n-1}-1$ is:

$$|(2^{2n}(2^{4n}-1))^{-1}|_{2^{2n-1}-1} = 2^{2n-2} + \sum_{l=1}^{2n-3} 2^l \quad (3.132)$$

where n is natural number(n>1), l is odd. The above expression contains n terms.

Examples: The following values of multiplicative inverse for different values of n are found using the program given in Appendix A (Section A.2).

The value of $|(2^{2n}(2^{4n}-1))^{-1}|_{2^{2n-1}-1}$ for different values of n is:

For $n = 2, |(2^{2n}(2^{4n}-1))^{-1}|_{2^{2n-1}-1} = |4080^{-1}|_7$=6

$$= (110)_2 \; in \; binary$$

$$= 2^1 + 2^2$$

For $n = 3, |(2^{2n}(2^{4n} - 1))^{-1}|_{2^{2n-1}-1} = |262080^{-1}|_{31}$=26

$$= (11010)_2$$

$$= 2^1 + 2^3 + 2^4$$

For $n = 4, |(2^{2n}(2^{4n} - 1))^{-1}|_{2^{2n-1}-1} = |16776960^{-1}|_{127}$=106

$$= (1101010)_2$$

$$= 2^1 + 2^3 + 2^5 + 2^6$$

For $n = 5, |(2^{2n}(2^{4n} - 1))^{-1}|_{2^{2n-1}-1} = |1073740800^{-1}|_{511}$=426

$$= (110101010)_2$$

$$= 2^1 + 2^3 + 2^5 + 2^7 + 2^8$$

Thus the above values of $|(2^{2n}(2^{4n} - 1))^{-1}|_{2^{2n-1}-1}$ can be generalized as follows,

$$|(2^{2n}(2^{4n} - 1))^{-1}|_{2^{2n-1}-1} = = 2^{2n-2} + \sum_{l=1}^{2n-3} 2^l$$

where n is natural number(n>1), *l* is is odd.

Calculation of $X^{(1)}$:

The converter design and proof for calculation of value of $X^{(1)}$ for four moduli set $\{2^{2n}, 2^{2n} + 1, 2^n + 1, 2^n - 1\}$ using New CRT I is given in [14]. The following equation from [14] is useful for the derivation of *X*.

$$X^{(1)} = = x_1 + 2^{2n}Z \tag{3.133}$$

Calculation of X:

The value of *X* is calculated from MRC as follows:

$$X = X^{(1)} + 2^{2n}(2^{4n} - 1)||(2^{2n}(2^{4n} - 1))^{-1}|_{2^{2n-1}-1} \cdot \left(x_5 - X^{(1)}\right)|_{2^{2n-1}-1}$$

$$= X^{(1)} + 2^{2n}(2^{4n} - 1)P \tag{3.134}$$

where

$$P = ||(2^{2n}(2^{2n}-1))^{-1}|_{2^{2n-1}-1}T|_{2^{2n-1}-1} \text{ and } T = |\left(x_5 - X^{(1)}\right)|_{2^{2n-1}-1} \quad (3.135)$$

$$T = |x_5 - x_1 - 2^n M|_{2^{2n-1}-1} = |a_1 + a_2 + a_3 + a_4 + a_5|_{2^{2n-1}-1} \quad (3.136)$$

$$a_1 = \underbrace{x_{5,2n-2}x_{5,2n-3}\dots x_{5,1}x_{5,0}}_{2n-1} \quad (3.137)$$

$$a_2 = \overline{\underbrace{x_{1,2n-2}\dots x_{1,1}x_{1,0}}_{2n-1}} \quad (3.138)$$

$$a_3 = \underbrace{1\dots 11}_{2n-4}\,\overline{\underbrace{Z_{4n-1}Z_{4n-2}}_{2}}\,\overline{\underbrace{x_{1,2n-1}}_{1}} \quad (3.139)$$

$$a_4 = \overline{\underbrace{Z_{4n-4}Z_{4n-5}\dots Z_{2n+1}Z_{2n}}_{2n-2}}\,\overline{\underbrace{Z_{4n-3}}_{1}} \quad (3.140)$$

$$a_5 = \overline{\underbrace{Z_{2n-3}Z_{2n-4}\dots Z_1Z_0}_{2n-2}}\,\overline{\underbrace{Z_{2n-2}}_{1}} \quad (3.141)$$

The value of *P* in equation (3.135) can be simplified by substituting value of equation (3.132) and operating circular left shift on bits of *T* as follows:

$$P = |CLS(T, 2n-2) + CLS(T, 1) + CLS(T, 3) + \cdots + CLS(T, 2n-3)|_{2^{2n-1}-1} \quad (3.142)$$

The value of *X* in the equation (3.134) can be simplified by substituting equation (3.133) as:

$$\begin{aligned} X &= X^{(1)} + 2^{2n}(2^{4n}-1)P = x_1 + 2^{2n}Z + 2^{2n}(2^{4n}-1)P \\ &= x_1 + 2^{2n}(Z + (2^{4n}-1)P) \\ &= x_1 + 2^{2n}Q \end{aligned} \quad (3.143)$$

where

$$Q = Z + (2^{4n}-1)P = Z + 2^{4n}P - P = K - P \quad (3.144)$$

$$K = Z + 2^{4n}P = \underbrace{P_{2n-2}P_{2n-3}\dots P_1P_0}_{2n-1}\,\underbrace{Z_{4n-1}Z_{4n-2}\dots Z_1Z_0}_{4n} \quad (3.145)$$

Also, since x_1 is a 2n-bit number, *X* in (3.143) can be obtained as

$$X = x_1 + 2^{2n}Q = \underbrace{Q_{6n-2}Q_{6n-3}\dots Q_1Q_0}_{6n-1}\,\underbrace{x_{1,2n-1}x_{1,2n-2}\dots x_{1,1}x_{1,0}}_{2n} \quad (3.146)$$

Example: Consider the moduli set $\{2^{2n}, 2^{2n}+1, 2^{n}+1, 2^{n}-1, 2^{2n-1}-1\}$ where n=3. The weighted number X can be calculated from its RNS representation (51, 31, 1, 5, 28) as follows:

For n=3 the moduli set is {64, 65, 9, 7, 31} and also residues have binary representation as below

$$x_1 = 51 = (110011)_2$$

$$x_2 = 31 = (0011111)_2$$

$$x_3 = 1 = (0001)_2$$

$$x_4 = 5 = (101)_2$$

$$x_5 = 28 = (11100)_2$$

The value of Z in (3.133) is calculated from converter of [14] and is given as:

$$Z = 2425 = (100101111001)_2$$

According to (3.137), (3.138), (3.139), (3.140), (3.141), (3.136), and (3.142) we have

$$a_1 = (11100)_2 = 28$$

$$a_2 = (01100)_2 = 12$$

$$a_3 = (11010)_2 = 26$$

$$a_4 = (01001)_2 = 9$$

$$a_5 = (01100)_2 = 12$$

$$T = |87|_{31} = (11001)_2 = 25$$

$$P = |650|_{31} = 30 = (11110)_2$$

Substituting the values of Z and P in Q, X can be calculated from (3.145), (3.144) and (3.146) as below

$$K = (11110100101111001)_2 = 125305$$

$$Q = 125305 - 30 = 125775$$

$$X = (11110101101001111110011)_2 = 8017651$$

We can see that $|8017651|_{64} = 51, |8017651|_{65} = 31,\ |8017651|_{65} = 1,\ |8017651|_7 = 5,$ $|8017651|_{31} = 28$ and therefore the calculated *X* is indeed the weighted value of the residue representation (51, 31, 1, 5, 28) with respect to the moduli set {64, 65, 9, 7, 31}.

Hardware Implementation: The reverse converter hardware architecture for the five moduli set $\{2^{2n}, 2^{2n}+1, 2^n+1, 2^n-1, 2^{2n-1}-1\}$ with corresponding residues $(x_1, x_2, x_3, x_4, x_5)$ of the integer *X* is shown in Fig. 3.5. Area and Delay specification for each part of the converter are shown in Table 3.5.

3.1.4.2 Reverse Converter Design for S_4 Using New CRT I and MRC (Method 2):

The set S_4 here is decomposed into two subsets $A_1 = \{2^{2n}, 2^{2n-1}-1\}$ and $A_2 = \{2^{2n}+1, 2^n-1, 2^n+1\}$. Two interim integers $X^{(1)}$ and $X^{(2)}$ are calculated from the residues x_1, x_2 of A_1 and x_3, x_4, x_5 of A_2. The conversion algorithms MRC and New CRT I are used to calculate $X^{(1)}$ and $X^{(2)}$ respectively. Next, the MRC algorithm is applied to calculate the integer *X* from the residues ($X^{(1)}$, $X^{(2)}$) corresponding to the moduli set $A_3 = \{2^{2n}(2^{2n-1}-1), 2^{4n}-1\}$. The following propositions are needed for the derivation of *X*.

Proposition 1: The multiplicative inverse of 2^{2n} modulo $2^{2n-1}-1$ is:

$$|m_1^{-1}|_{m_2} = |(2^{2n})^{-1}|_{2^{2n-1}-1} = 2^{2n-2} \tag{3.147}$$

where n is natural number larger than 1.

Proof: Using property of equation (1.35), if $|a^{-1}|_m = b$ then $|a \cdot b|_m = 1$

Since $|(2^{2n})^{-1}|_{2^{2n-1}-1} = 2^{2n-2}$, we have

Table 3.5

Area and Delay Specification of Reverse Converter for the moduli set S_4 using New CRT I and MRC (Method 1)

Parts	**FA**	**NOT**	**XOR/AND pairs**	**XNOR/OR pairs**	**Delay**
OPU 1		6n-1			t_{NOT}
CSA1	3			2n-4	t_{FA}
CSA2	2n-1				t_{FA}
CSA3	2n-1				t_{FA}
CPA1	2n-1				$(4n-2)t_{FA}$
OPU2	-				-
CSA4 Tree	$2n^2$-5n+2				$l \cdot t_{FA}$
CPA2	2n-1				$(4n-2)\ t_{FA}$
OPU3		2n-1			t_{NOT}
CPA4	2n-1			4n	$(6n-1)t_{FA}$
Area of Converter 2 [14]		(10n+6)A_{FA}+ (6n+3)A_{NOT}+ (4n-3)A_{XOR}+ (4n-3)A_{AND}+ (2n-3)A_{XNOR}+ (2n-3)A_{OR}			
Delay of Converter 2 [14]		(8n+3)t_{FA} + t_{NOT}			
Total Area		($2n^2$ +15n+6)A_{FA}+ (14n+1)A_{NOT}+ (4n-3)A_{XOR}+ (4n-3)A_{AND}+ (8n-7)A_{XNOR}+ (8n-7)A_{OR}			
Total Delay		(22n+1+*l*)t_{FA} + 3t_{NOT}			

Here *l* is the minimum number of levels of CSA tree required to process (n) input operands.

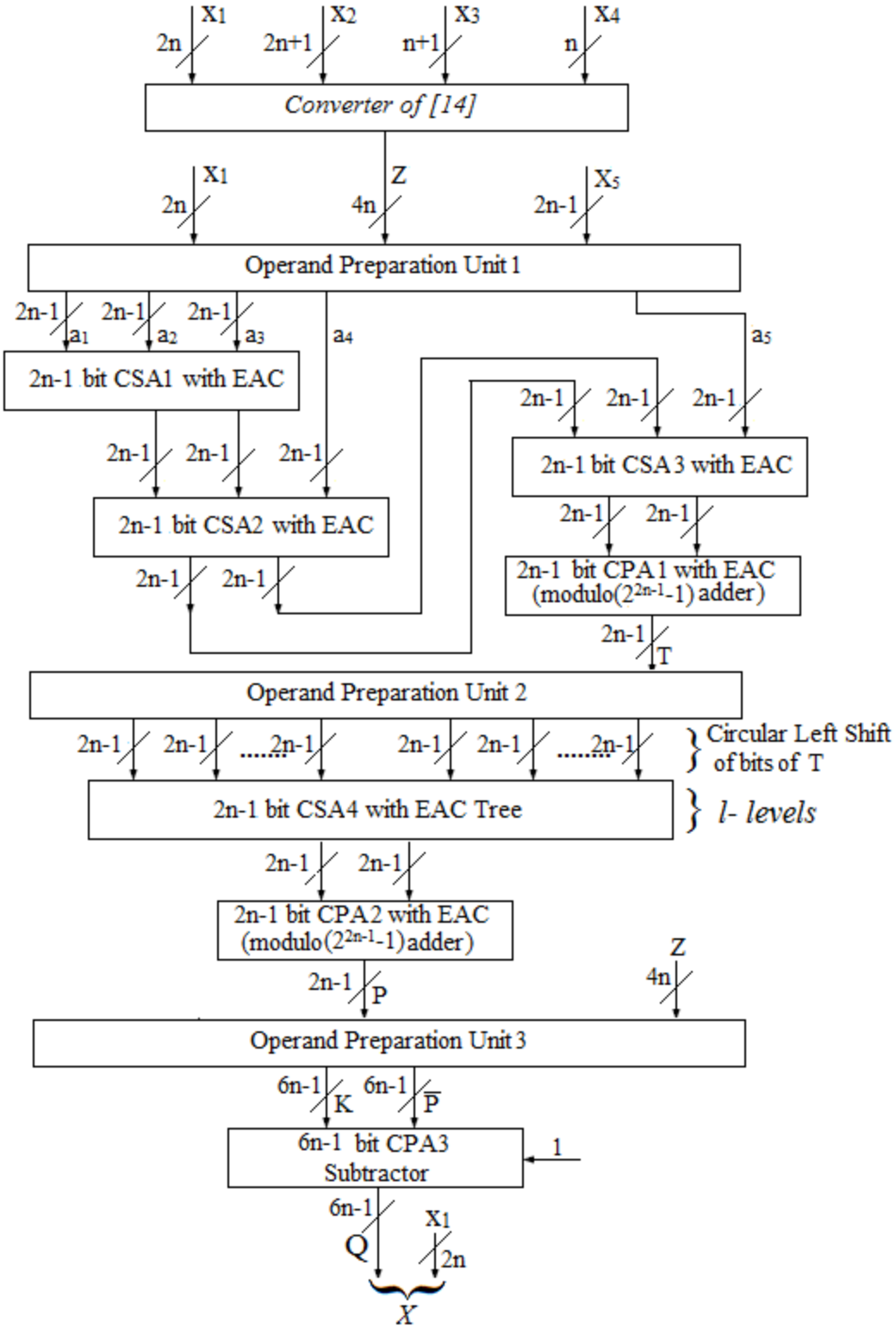


Figure 3.5 Reverse Converter for the moduli set S_4 using New CRT I and MRC (Method 1)

$$|2^{2n} \cdot 2^{2n-2}|_{2^{2n-1}-1} = |2 \cdot 2^{2n-2}|_{2^{2n-1}-1} = |2^{2n-1}|_{2^{2n-1}-1} = 1$$

Proposition 2: The multiplicative inverse of $2^{2n}(2^{2n-1}-1)$ modulo $2^{4n}-1$ is:

$$|(2^{2n}(2^{2n-1}-1))^{-1}|_{2^{4n}-1} = \sum_{l=2}^{2n} 2^l + \sum_{m=2n+3}^{4n-1} 2^m \qquad (3.148)$$

where n is natural number(n>1), *l* is even, *m* is odd. The above expression contains $(2n-1)$ terms.

Examples: The following values of multiplicative inverse for different values of n are found using the program given in Appendix A (Section A.2).

The value of $|(2^{2n}(2^{2n-1}-1))^{-1}|_{2^{4n}-1}$ for different values of n is:

For $n = 2, |(2^{2n}(2^{2n-1}-1))^{-1}|_{2^{4n}-1} = |112^{-1}|_{255}$=148

$$= (10010100)_2 \; in \; binary$$

$$= 2^2 + 2^4 + 2^7$$

For $n = 3, |(2^{2n}(2^{2n-1}-1))^{-1}|_{2^{4n}-1} = |1984^{-1}|_{4095}$=2644

$$= (101001010100)_2$$

$$= 2^2 + 2^4 + 2^6 + 2^9 + 2^{11}$$

For $n = 4, |(2^{2n}(2^{2n-1}-1))^{-1}|_{2^{4n}-1} = |32512^{-1}|_{65535}$=43348

$$= (1010100101010100)_2$$

$$= 2^2 + 2^4 + 2^6 + 2^8 + 2^{11} + 2^{13} + 2^{15}$$

For $n = 5, |(2^{2n}(2^{2n-1}-1))^{-1}|_{2^{4n}-1} = |523264^{-1}|_{1048575}$=697684

$$= (10101010010101010100)_2$$

$$= 2^2 + 2^2 + 2^6 + 2^8 + 2^{10} + 2^{13} + 2^{15} + 2^{17} + 2^{19}$$

Thus the above values of $|(2^{2n}(2^{2n-1}-1))^{-1}|_{2^{4n}-1}$ can be generalized as follows,

$$|(2^{2n}(2^{2n-1}-1))^{-1}|_{2^{4n}-1} = \sum_{l=2}^{2n} 2^l + \sum_{m=2n+3}^{4n-1} 2^m$$

where n is natural number(n>1), *l* is even, *m* is odd.

Calculation of $X^{(1)}$*:*

The value of $X^{(1)}$ is calculated from MRC as follows:

$$X^{(1)} = x_1 + m_1 \cdot |\,|m_1^{-1}|_{m_2} \cdot (x_2 - x_1)\,|_{m_2} \tag{3.149}$$

Substituting the value (3.147), m_1 and m_2 in (3.105) we have

$$X^{(1)} = x_1 + 2^{2n} \cdot |\,2^{2n-2} \cdot (x_2 - x_1)\,|_{2^{2n-1}-1}$$

$$= x_1 + 2^{2n}M \tag{3.150}$$

where

$$M = |a_1 + a_2 + a_3|_{2^{2n-1}-1} \tag{3.151}$$

$$a_1 = \underbrace{x_{2,0}}_{1}\underbrace{x_{2,2n-2}x_{2,2n-3}\dots x_{2,1}}_{2n-2} \tag{3.152}$$

$$a_2 = \underbrace{\overline{x_{1,2n-1}}}_{1}\underbrace{1\dots 11}_{2n-2} \tag{3.153}$$

$$a_3 = \underbrace{\overline{x_{1,0}}}_{1}\underbrace{\overline{x_{1,2n-2}x_{1,2n-3}\dots x_{1,1}}}_{2n-2} \tag{3.154}$$

Calculation of $X^{(2)}$*:*

The value of $X^{(2)}$ is calculated from New CRT I using the equations (3.110) to (3.116).

Calculation of X:

The value of *X* is calculated from MRC as follows:

$$X = X^{(1)} + 2^{2n}(2^{2n-1}-1)||(2^{2n}(2^{2n-1}-1))^{-1}|_{2^{4n}-1} \cdot \left(X^{(2)} - X^{(1)}\right)|_{2^{4n}-1}$$

$$= X^{(1)} + 2^{2n}(2^{2n-1}-1)P \tag{3.155}$$

where

$$P = ||(2^{2n}(2^{2n-1}-1))^{-1}|_{2^{4n}-1}T|_{2^{4n}-1} \text{ and } T = |\left(X^{(2)} - X^{(1)}\right)|_{2^{4n}-1} \quad (3.156)$$

$$T = |x_3 + (2^{2n}+1)N - x_1 - 2^{2n}M|_{2^{4n}-1} = |a_4 + a_5 + a_6|_{2^{4n}-1} \quad (3.157)$$

$$a_4 = \underbrace{0 \dots 00}_{2n-1}\underbrace{x_{3,2n}x_{3,2n-1} \dots x_{3,1}x_{3,0}}_{2n+1} \quad (3.158)$$

$$a_5 = \underbrace{N_{2n-1}N_{2n-2} \dots N_1N_0}_{2n}\underbrace{N_{2n-1}N_{2n-2} \dots N_1N_0}_{2n} \quad (3.159)$$

$$a_6 = \underbrace{1}_{1}\overline{\underbrace{M_{2n-2}M_{2n-3} \dots M_1M_0}_{2n-1}}\overline{\underbrace{x_{1,2n-1}x_{1,2n-2} \dots x_{1,1}x_{1,0}}_{2n}} \quad (3.160)$$

The value of *P* in equation (3.156) can be simplified by substituting value of equation (3.148) and operating circular left shift on bits of *T* as follows:

$$P = |CLS(T,2) + CLS(T,4) + \cdots + CLS(T,2n) + CLS(T,2n+3) +$$
$$+CLS(T,2n+5) \cdots + CLS(T,4n-1)|_{2^{4n}-1} \quad (3.161)$$

The value of *X* in the equation (3.155) can be simplified by substituting equation (3.150) as:

$$X = X^{(1)} + 2^{2n}(2^{2n-1}-1)P = x_1 + 2^{2n}M + 2^{2n}(2^{2n-1}-1)P$$
$$= x_1 + 2^{2n}(M + (2^{2n-1}-1)P)$$
$$= x_1 + 2^{2n}Q \quad (3.162)$$

where

$$Q = M + (2^{2n-1}-1)P = M + 2^{2n-1}P - P = K - P \quad (3.163)$$

$$K = M + 2^{2n-1}P = \underbrace{P_{4n-1}P_{4n-2} \dots P_1P_0}_{4n}\underbrace{M_{2n-2}M_{2n-3} \dots M_1M_0}_{2n-1} \quad (3.164)$$

Also, since x_1 is a 2n-bit number, *X* in (3.162) can be obtained as

$$X = x_1 + 2^{2n}Q = \underbrace{Q_{6n-2}Q_{6n-3} \dots Q_1Q_0}_{6n-1}\underbrace{x_{1,2n-1}x_{1,2n-2} \dots x_{1,1}x_{1,0}}_{2n} \quad (3.165)$$

Example: Consider the moduli set $\{2^{2n}, 2^{2n-1}-1, 2^{2n}+1, 2^n-1, 2^n+1\}$ where n=4. The weighted number *X* can be calculated from its RNS representation (183, 50, 103, 1, 14) as follows:

For n=4 the moduli set is {256, 127, 257, 15, 17} and also residues have binary representation as below

$$x_1 = 183 = (10110111)_2$$

$$x_2 = 50 = (0110010)_2$$

$$x_3 = 103 = (001100111)_2$$

$$x_4 = 1 = (0001)_2$$

$$x_5 = 14 = (01110)_2$$

According to (3.108), (3.109), (3.107), (3.113), (3.114), (3.115), (3.116), (3.112), (3.120), (3.121), (3.122), (3.119), and (3.118) we have

$$a_1 = (0011001)_2 = 25$$

$$a_2 = (0111111)_2 = 63$$

$$a_3 = (0100100)_2 = 36$$

$$M = |124|_{127} = (1111100)_2 = 124$$

$$N = |-12276|_{255} = (11011011)_2 = 219$$

$$a_4 = (0000000001100111)_2 = 103$$

$$a_5 = (1101101111011011)_2 = 56283$$

$$a_6 = (1000001101001000)_2 = 33608$$

$$T = |89994|_{65535} = 24459 = (101111110001011)_2$$

$$P = |1060248732|_{65535} = 23502 = (101101111001110)_2$$

Substituting the values of *M* and *P* in *Q*, *X* can be calculated from (3.164), (3.163) and (3.165) as below

$$K = (10110111100111011111100)_2 = 3008380$$

$$Q = 3008380 - 23502 = 2984878$$

$$X = (10110110001011101010111010110111)_2 = 764128951$$

We can see that $|764128951|_{256} = 183$, $|764128951|_{127} = 50$, $|764128951|_{257} = 103$, $|764128951|_{15} = 1$, $|764128951|_{17} = 14$ and therefore the calculated X is indeed the weighted value of the residue representation (183, 50, 103, 1, 14) with respect to the moduli set {256, 127, 257, 15, 17}.

Hardware Implementation: The reverse converter hardware architecture for the five moduli set $\{2^{2n}, 2^{2n}+1, 2^n+1, 2^n-1, 2^{2n-1}-1\}$ with corresponding residues $(x_1, x_2, x_3, x_4, x_5)$ of the integer X is shown in Fig. 3.6. Area and Delay specification for each part of the converter are shown in Table 3.6.

3.1.5 Reverse Converter Design for $S_5 = \{2^{4n}+1, 2^{2n}+1, 2^n-1, 2^n, 2^n+1\}$:

Consider the five moduli set $S_5 = \{2^n,\ 2^{4n}+1,\ 2^{2n}+1, 2^n+1,\ 2^n-1\} = \{m_1, m_2, m_3, m_4, m_5\}$, where n is a natural number (n>2) and let the corresponding residues of the integer X be $(x_1, x_2, x_3, x_4, x_5)$. The residues have bit-level representations as:

$$x_1 = (x_{1,n-1}x_{1,n-2} \dots x_{1,1}x_{1,0})_2 \quad (3.166)$$

$$x_2 = (x_{2,4n}x_{2,4n-1} \dots x_{2,1}x_{2,0})_2 \quad (3.167)$$

$$x_3 = (x_{3,2n}x_{3,2n-1} \dots x_{3,1}x_{3,0})_2 \quad (3.168)$$

$$x_4 = (x_{4,n}x_{4,n-1} \dots x_{4,1}x_{4,0})_2 \quad (3.169)$$

$$x_5 = (x_{5,n-1}x_{5,n-2} \dots x_{5,1}x_{5,0})_2 \quad (3.170)$$

The following section describe the design of reverse converter for S_5 using New CRT I conversion algorithm.

3.1.5.1 Reverse Converter Design for S_5 Using New CRT I:

Table 3.6

Area and Delay Specification of Reverse Converter for the moduli set S_4 using New CRT I and MRC (Method 2)

Parts	**FA**	**NOT**	**XOR/AND pairs**	**XNOR/OR pairs**	**MUX**	**Delay**
OPU 1		5n+1			1 (2n) bit	$t_{NOT} + t_{MUX}$
CSA1	1			2n-2		t_{FA}
CPA1	2n-1					$(4n-2)t_{FA}$
CSA2	n+1		n-1			t_{FA}
CSA3	n+1			n-1		t_{FA}
CPA2	2n					$4n\ t_{FA}$
OPU2		4n-1				t_{NOT}
CSA4	2n+1		2n-1			t_{FA}
CPA3	4n					$8n\ t_{FA}$
OPU3	-					-
CSA5 Tree	$8n^2$-12n					$l \cdot t_{FA}$
CPA4	4n					$8n\ t_{FA}$
OPU4		4n				t_{NOT}
CPA5	4n			2n-1		$(6n-1)t_{FA}$
Total Area		$(8n^2+8n+3)A_{FA}$+ $(13n)A_{NOT}$+ $(3n-2)A_{XOR}$+ $(3n-2)A_{AND}$+ $(5n-4)A_{XNOR}$+ $(5n-4)A_{OR}$ + $A_{MUX(2n)}$				
Total Delay		$(26n+2+l)t_{FA}$ + $3t_{NOT}$ + t_{MUX}				

Here l is the minimum number of levels of CSA tree required to process (2n-1) input operands.

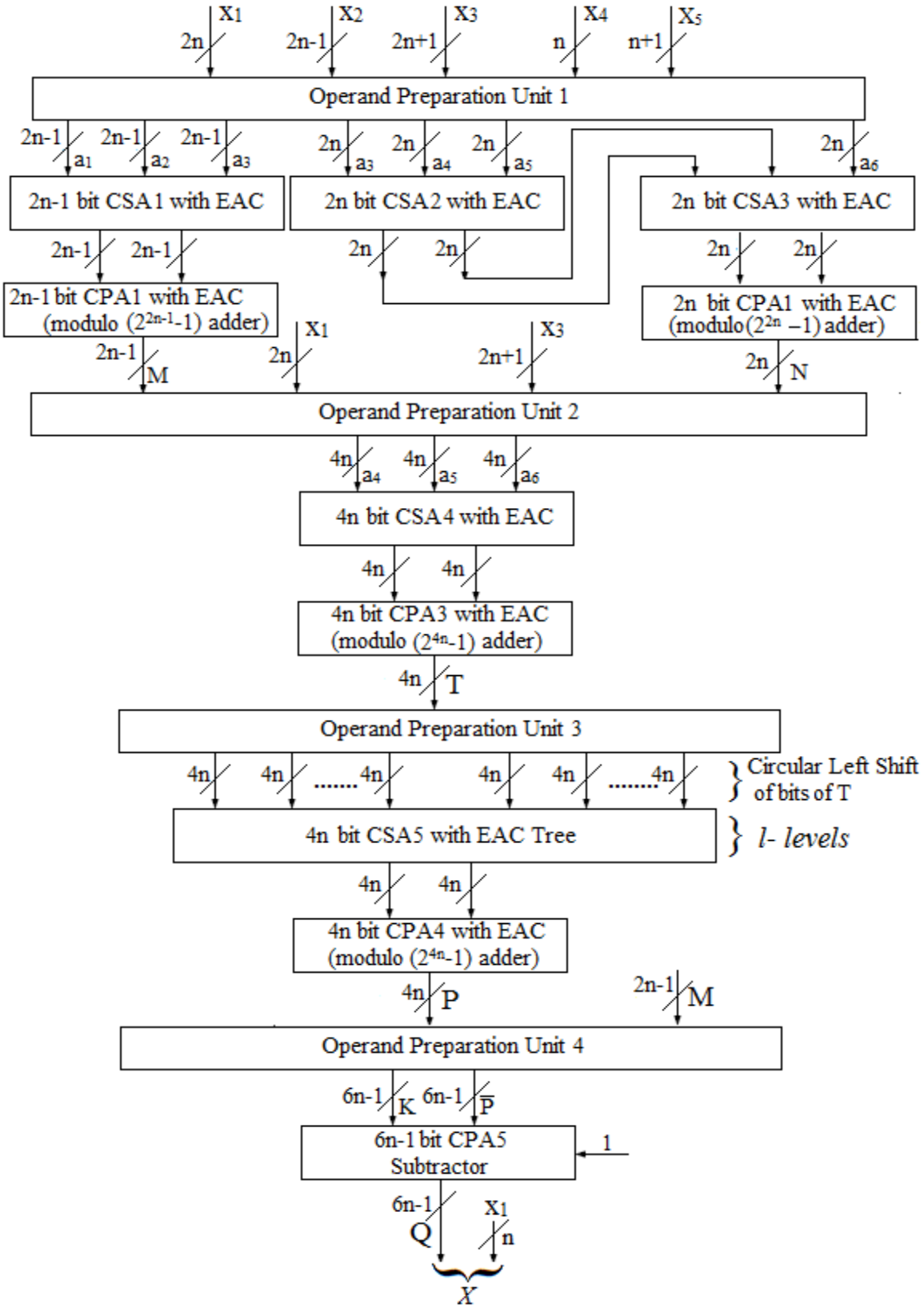


Figure 3.6 Reverse Converter for the moduli set S_4 using New CRT I and MRC (Method 2)

The value of X is calculated from New CRT I as shown below:

$$X = x_1 + m_1|\, k_1(x_2 - x_1) +$$

$$k_2 m_2(x_3 - x_2) + k_3 m_2 m_3(x_4 - x_3) + k_4 m_2 m_3 m_4(x_5 - x_4)|_{m_2 m_3 m_4 m_5} \quad (3.171)$$

where

$$k_1 = |m_1^{-1}|_{m_2 m_3 m_4 m_5},\ k_2 = |(m_1 m_2)^{-1}|_{m_3 m_4 m_5},\ k_3 = |(m_1 m_2 m_3)^{-1}|_{m_4 m_5} \text{and}$$

$$k_4 = |(m_1 m_2 m_3 m_4)^{-1}|_{m_5} \quad (3.172)$$

The following propositions are needed for the derivation of *X*.

Proposition 1: The multiplicative inverse of 2^n modulo $2^{8n} - 1$ is:

$$|m_1^{-1}|_{m_2 m_3 m_4 m_5} = |(2^n)^{-1}|_{2^{8n}-1} = 2^{7n} \quad (3.173)$$

where n is natural number larger than 2.

Proof: Using property of equation (1.35), if $|a^{-1}|_m = b$ then $|\, a \cdot b\,|_m = 1$

Since $|(2^n)^{-1}|_{2^{8n}-1} = 2^{7n}$, we have

$$|2^n \cdot 2^{7n}|_{2^{8n}-1} = |2^{8n}|_{2^{8n}-1} = |2^{8n}|_{2^{8n}-1} = 1$$

Proposition 2: The multiplicative inverse of $2^n(2^{4n} + 1)$ modulo $2^{4n} - 1$ is:

$$|(m_1 m_2)^{-1}|_{m_3 m_4 m_5} = |(2^n(2^{4n} + 1))^{-1}|_{2^{4n}-1} = 2^{3n-1} \quad (3.174)$$

where n is natural number larger than 2.

Proof: Using property of equation (1.35), if $|a^{-1}|_m = b$ then $|\, a \cdot b\,|_m = 1$

Since $|(2^n(2^{4n} + 1))^{-1}|_{2^{4n}-1} = 2^{3n-1}$, we have

$$|2^n(2^{4n} + 1) \cdot 2^{3n-1}|_{2^{4n}-1} = |2^n(2) \cdot 2^{3n-1}|_{2^{4n}-1} = |2^{4n}|_{2^{4n}-1} = 1$$

Proposition 3: The multiplicative inverse of $2^n(2^{4n} + 1)(2^{2n} + 1)$ modulo $2^{2n} - 1$ is:

$$|(m_1 m_2 m_3)^{-1}|_{m_4 m_5} = |(2^n(2^{4n} + 1)(2^{2n} + 1))^{-1}|_{2^{2n}-1} = 2^{n-2} \quad (3.175)$$

where n is natural number larger than 2.

Proof: Using property of equation (1.35), if $|a^{-1}|_m = b$ then $|\, a \cdot b\,|_m = 1$

Since$|(2^n(2^{4n}+1)(2^{2n}+1))^{-1}|_{2^{2n}-1} = 2^{n-2}$, we have

$$|2^n(2^{4n}+1)(2^{2n}+1)\cdot 2^{n-2}|_{2^{2n}-1} = |2^n(2)(2)\cdot 2^{n-2}|_{2^{2n}-1} = |2^{2n}|_{2^{2n}-1} = 1$$

Proposition 4: The multiplicative inverse of $2^n(2^{4n}+1)(2^{2n}+1)(2^n+1)$ modulo 2^n-1 is:

$$|(m_1m_2m_3m_4)^{-1}|_{m_5} = |(2^n(2^{4n}+1)(2^{2n}+1)(2^n+1))^{-1}|_{2^n-1} = 2^{n-3} \tag{3.176}$$

where n is natural number larger than 2.

Proof: Using property of equation (1.35), if $|a^{-1}|_m = b$ then $|a\cdot b|_m = 1$

Since$|(2^n(2^{4n}+1)(2^{2n}+1)(2^n+1))^{-1}|_{2^n-1} = 2^{n-3}$, we have

$$|2^n(2^{4n}+1)(2^{2n}+1)(2^n+1)\cdot 2^{n-3}|_{2^n-1} = |2^n(2)(2)(2)\cdot 2^{n-3}|_{2^n-1} = |2^{2n}|_{2^n-1} = 1$$

Substituting the values of (3.173), (3.172), (3.173), and (3.174) in (3.171), the value of X can be simplified as:

$$X = x_1 + 2^nM \tag{3.177}$$

where

$$M = |a_1 + a_2 + a_3 + a_4 + a_5 + a_6 + a_7|_{2^{8n}-1} \tag{3.178}$$

$$a_1 = \underbrace{x_{5,2}x_{5,1}x_{5,0}}_{3}\underbrace{x_{5,n-1}\dots x_{5,0}}_{n}\underbrace{x_{5,n-1}\dots x_{5,0}}_{n}\underbrace{x_{5,n-1}\dots x_{5,0}}_{n}\underbrace{x_{5,n-1}\dots x_{5,0}}_{n}$$

$$\underbrace{x_{5,n-1}\dots x_{5,0}}_{n}\underbrace{x_{5,n-1}\dots x_{5,0}}_{n}\underbrace{x_{5,n-1}\dots x_{5,0}}_{n}\underbrace{x_{5,n-1}\dots x_{5,3}}_{n-3} \tag{3.179}$$

$$a_2 = \underbrace{\overline{x_{1,n-1}x_{1,n-2}\dots x_{1,1}x_{1,0}}}_{n}\underbrace{\overline{x_{2,4n}x_{2,4n-1}\dots x_{2,1}x_{2,0}}}_{4n+1}\underbrace{1\dots 11}_{3n-1} \tag{3.180}$$

$$a_3 = \underbrace{1\dots 11}_{n+1}\underbrace{\overline{x_{3,2n}x_{3,2n-1}\dots x_{3,1}x_{3,0}}}_{2n+1}\underbrace{1\dots 11}_{2n-1}\underbrace{\overline{x_{3,2n}x_{3,2n-1}\dots x_{3,1}x_{3,0}}}_{2n+1}\underbrace{1\dots 11}_{n-2} \tag{3.181}$$

$$a_4 = \underbrace{\overline{x_{4,2}x_{4,1}x_{4,0}}}_{3}\underbrace{1\dots 11}_{n-1}\underbrace{\overline{x_{4,n}\dots x_{4,0}}}_{n+1}\underbrace{1\dots 11}_{n-1}\underbrace{\overline{x_{4,n}\dots x_{4,0}}}_{n+1}\underbrace{1\dots 11}_{n-1}\underbrace{\overline{x_{4,n}\dots x_{4,0}}}_{n+1}\underbrace{1\dots 11}_{n-1}\underbrace{\overline{x_{4,n}\dots x_{4,3}}}_{n-2}$$

(3.182)

$$a_5 = \underbrace{00}_{2}\underbrace{x_{4,n}\dots x_{4,0}}_{n+1}\underbrace{0\dots 00}_{n-1}\underbrace{x_{4,n}\dots x_{4,0}}_{n+1}\underbrace{0\dots 00}_{n-1}\underbrace{x_{4,n}\dots x_{4,0}}_{n+1}\underbrace{0\dots 00}_{n-1}\underbrace{x_{4,n}\dots x_{4,0}}_{n+1}\underbrace{0\dots 00}_{n-3}$$

(3.183)

$$a_6 = \underbrace{x_{2,n}x_{2,n-1}\dots x_{2,0}}_{n+1}\underbrace{0\dots00}_{4n-1}\underbrace{x_{2,4n}x_{2,4n-1}\dots x_{2,n+2}}_{3n} \tag{3.184}$$

$$a_7 = \underbrace{x_{3,n+1}\dots x_{3,0}}_{n+2}\underbrace{0\dots00}_{2n-1}\underbrace{x_{3,2n}\dots x_{3,0}}_{2n+1}\underbrace{0\dots00}_{2n-1}\underbrace{x_{3,2n}\dots x_{3,n+2}}_{n-1} \tag{3.185}$$

Also, since x_1 is an n-bit number, *X* in (3.177) can be obtained as

$$X = x_1 + 2^n M = \underbrace{M_{8n-1}M_{8n-2}\dots M_1M_0}_{8n}\underbrace{x_{1,n-1}x_{1,n-2}\dots x_{1,1}x_{1,0}}_{n} \tag{3.186}$$

Example: Consider the moduli set $\{2^n,\ 2^{4n}+1,\ 2^{2n}+1, 2^n+1,\ 2^n-1\}$ where n=3. The weighted number *X* can be calculated from its RNS representation (4, 676, 22, 4, 1) as follows:

For n=3 the moduli set is {8, 4097, 65, 9, 7} and also residues have binary representation as below

$$x_1 = 183 = (10110111)_2$$

$$x_2 = 50 = (0110010)_2$$

$$x_3 = 103 = (001100111)_2$$

$$x_4 = 1 = (0001)_2$$

$$x_5 = 14 = (01110)_2$$

According to (3.179), (3.180), (3.181), (3.182), (3.183), (3.184), (3.185), and (3.178) we have

$$a_1 = (001001001001001001001001)_2 = 2396745$$

$$a_2 = (011111010101101111111111)_2 = 8215551$$

$$a_3 = (111111010011111111010011)_2 = 16596947$$

$$a_4 = (011111011111011111011111)_2 = 8255455$$

$$a_5 = (000100000100000100000100)_2 = 1065220$$

$$a_6 = (010000000000000000101010)_2 = 4194346$$

$$a_7 = (101100000000101100000000)_2 = 11537152$$

$$M = |52261416|_{16777215} = (11101011100100010101 1)_2 = 1929771$$

Substituting the value of *M* in (3.186), *X* can be calculated as below

$$X = (111010111001000101011100)_2 = 15438172$$

We can see that $|15438172|_8 = 4$, $|15438172|_{4097} = 676$, $|15438172|_{65} = 22$, $|15438172|_9 = 4$, $|15438172|_7 = 1$ and therefore the calculated *X* is indeed the weighted value of the residue representation (4, 676, 22, 4, 1) with respect to the moduli set {8, 4097, 65, 9, 7}.

Hardware Implementation: The reverse converter hardware architecture for the five moduli set $\{2^n,\ 2^{4n}+1,\ 2^{2n}+1, 2^n+1,\ 2^n-1\}$ with corresponding residues $(x_1, x_2, x_3, x_4, x_5)$ of the integer *X* is shown in Fig. 3.7. Area and Delay specification for each part of the converter are shown in Table 3.7.

3.1.6 Reverse Converter Design for $S_6 = \{2^{4n}+1, 2^{2n}+1, 2^n-1, 2^{2n}, 2^n+1\}$:

Consider the five moduli set $S_6 = \{2^{2n},\ 2^{4n}+1,\ 2^{2n}+1, 2^n+1,\ 2^n-1\} = \{m_1, m_2, m_3, m_4, m_5\}$, where n is a natural number (n>1) and let the corresponding residues of the integer *X* be $(x_1, x_2, x_3, x_4, x_5)$. The residues have bit-level representations as:

$$x_1 = (x_{1,2n-1}x_{1,2n-2} \dots x_{1,1}x_{1,0})_2 \quad (3.187)$$

$$x_2 = (x_{2,4n}x_{2,4n-1} \dots x_{2,1}x_{2,0})_2 \quad (3.188)$$

$$x_3 = (x_{3,2n}x_{3,2n-1} \dots x_{3,1}x_{3,0})_2 \quad (3.189)$$

$$x_4 = (x_{4,n}x_{4,n-1} \dots x_{4,1}x_{4,0})_2 \quad (3.190)$$

$$x_5 = (x_{5,n-1}x_{5,n-2} \dots x_{5,1}x_{5,0})_2 \quad (3.191)$$

Table 3.7

Area and Delay Specifications of Reverse Converter for the moduli set S_5 using New CRT I

Parts	**FA**	**NOT**	**XOR/AND pairs**	**XNOR/OR pairs**	**Delay**
OPU1		8n+3			t_{NOT}
CSA1	n+2		4n-1	3n-1	t_{FA}
CSA2	4		2n-2	6n-2	t_{FA}
CSA3	4n+2		4n-2		t_{FA}
CSA4	8n				t_{FA}
CSA5	8n				t_{FA}
CPA1	8n				$16n\ t_{FA}$
Total Area	(29n+8)A_{FA}+ (8n+3)A_{NOT}+ (10n-5)A_{XOR}+ (10n-5)A_{AND}+ (9n-3)A_{XNOR}+ (9n-3)A_{OR}				
Total Delay	(16n+4)t_{FA} + t_{NOT}				

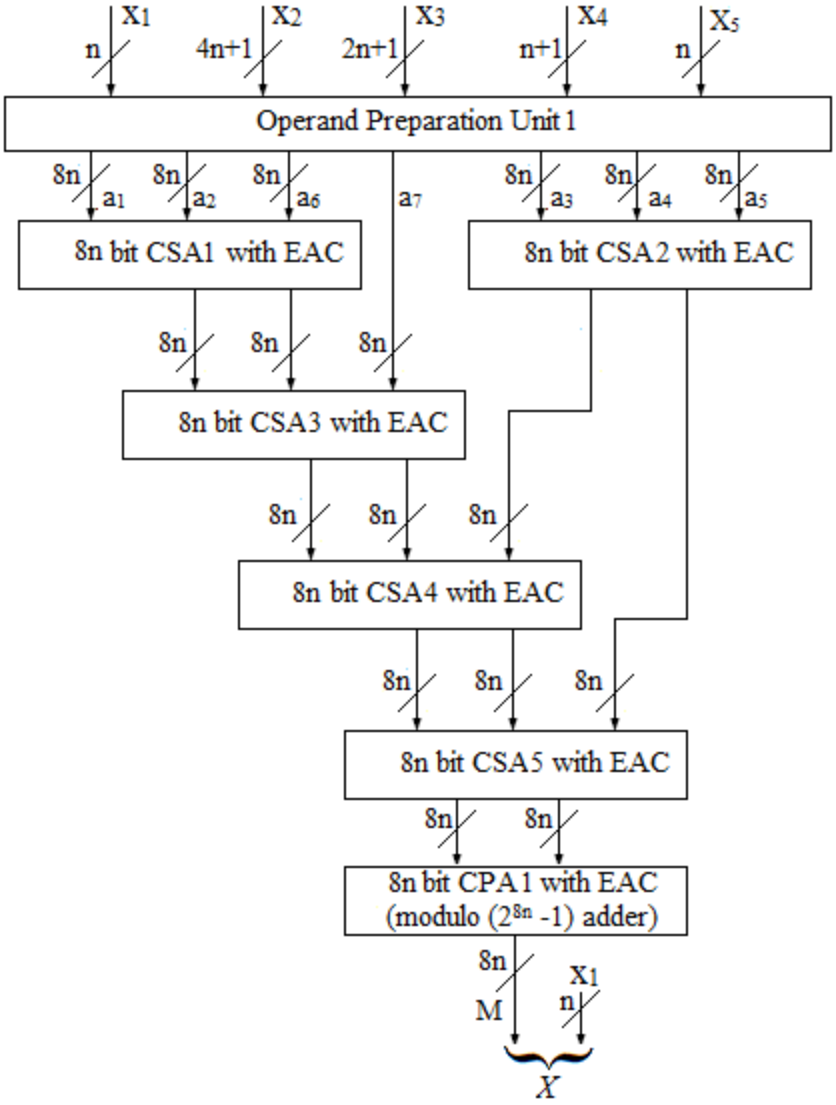


Figure 3.7 Reverse Converter for the moduli set S_5 using New CRT I

The following section describe the design of reverse converter for S_6 using New CRT I conversion algorithm.

3.1.6.1 Reverse Converter Design for S_6 Using New CRT I:

The value of X is calculated from New CRT I as shown below:

$$X = x_1 + m_1 | k_1(x_2 - x_1) +$$

$$k_2 m_2(x_3 - x_2) + k_3 m_2 m_3(x_4 - x_3) + k_4 m_2 m_3 m_4(x_5 - x_4)|_{m_2 m_3 m_4 m_5} \quad (3.192)$$

where

$$k_1 = |m_1^{-1}|_{m_2 m_3 m_4 m_5},\ k_2 = |(m_1 m_2)^{-1}|_{m_3 m_4 m_5},\ k_3 = |(m_1 m_2 m_3)^{-1}|_{m_4 m_5} \text{and}$$

$$k_4 = |(m_1 m_2 m_3 m_4)^{-1}|_{m_5} \quad (3.193)$$

The following propositions are needed for the derivation of *X*.

Proposition 1: The multiplicative inverse of 2^{2n} modulo $2^{8n} - 1$ is:

$$|m_1^{-1}|_{m_2 m_3 m_4 m_5} = |(2^{2n})^{-1}|_{2^{8n}-1} = 2^{6n} \quad (3.194)$$

where n is natural number larger than 1.

Proof: Using property of equation (1.35), if $|a^{-1}|_m = b$ then $|a \cdot b|_m = 1$

Since $|(2^{2n})^{-1}|_{2^{8n}-1} = 2^{6n}$, we have

$$|2^{2n} \cdot 2^{6n}|_{2^{8n}-1} = |2^{8n}|_{2^{8n}-1} = |2^{8n}|_{2^{8n}-1} = 1$$

Proposition 2: The multiplicative inverse of $2^{2n}(2^{4n} + 1)$ modulo $2^{4n} - 1$ is:

$$|(m_1 m_2)^{-1}|_{m_3 m_4 m_5} = |(2^{2n}(2^{4n} + 1))^{-1}|_{2^{4n}-1} = 2^{2n-1} \quad (3.195)$$

where n is natural number larger than 1.

Proof: Using property of equation (1.35), if $|a^{-1}|_m = b$ then $|a \cdot b|_m = 1$

Since $|(2^{2n}(2^{4n} + 1))^{-1}|_{2^{4n}-1} = 2^{2n-1}$, we have

$$|2^{2n}(2^{4n} + 1) \cdot 2^{2n-1}|_{2^{4n}-1} = |2^{2n}(2) \cdot 2^{2n-1}|_{2^{4n}-1} = |2^{4n}|_{2^{4n}-1} = 1$$

Proposition 3: The multiplicative inverse of $2^{2n}(2^{4n}+1)(2^{2n}+1)$ modulo $2^{2n}-1$ is:

$$|(m_1m_2m_3)^{-1}|_{m_4m_5} = |(2^{2n}(2^{4n}+1)(2^{2n}+1))^{-1}|_{2^{2n}-1} = 2^{2n-2} \tag{3.196}$$

where n is natural number larger than 1.

Proof: Using property of equation (1.35), if $|a^{-1}|_m = b$ then $|a \cdot b|_m = 1$

Since$|(2^{2n}(2^{4n}+1)(2^{2n}+1))^{-1}|_{2^{2n}-1} = 2^{2n-2}$, we have

$$|2^{2n}(2^{4n}+1)(2^{2n}+1)\cdot 2^{2n-2}|_{2^{2n}-1} = |2^{2n}(2)(2)\cdot 2^{2n-2}|_{2^{2n}-1} = |2^{4n}|_{2^{2n}-1} = 1$$

Proposition 4: The multiplicative inverse of $2^{2n}(2^{4n}+1)(2^{2n}+1)(2^{n}+1)$ modulo $2^{n}-1$ is:

$$|(m_1m_2m_3m_4)^{-1}|_{m_5} = |(2^{2n}(2^{4n}+1)(2^{2n}+1)(2^{n}+1))^{-1}|_{2^{n}-1} = 2^{2n-3} \tag{3.197}$$

where n is natural number larger than 1.

Proof: Using property of equation (1.35), if $|a^{-1}|_m = b$ then $|a \cdot b|_m = 1$

Since$|(2^{2n}(2^{4n}+1)(2^{2n}+1)(2^{n}+1))^{-1}|_{2^{n}-1} = 2^{2n-3}$, we have

$$|2^{2n}(2^{4n}+1)(2^{2n}+1)(2^{n}+1)\cdot 2^{n-3}|_{2^{n}-1} = |2^{2n}(2)(2)(2)\cdot 2^{n-3}|_{2^{n}-1} = |2^{3n}|_{2^{n}-1} = 1$$

Substituting the values of (3.194), (3.195), (3.196), and (3.197) in (3.192), the value of X can be simplified as:

$$X = x_1 + 2^{2n}M \tag{3.198}$$

where

$$M = |a_1 + a_2 + a_3 + a_4 + a_5 + a_6 + a_7|_{2^{8n}-1} \tag{3.199}$$

$$a_1 = \underbrace{x_{5,2}x_{5,1}x_{5,0}}_{3}\underbrace{x_{5,n-1}\dots x_{5,0}}_{n}\underbrace{x_{5,n-1}\dots x_{5,0}}_{n}\underbrace{x_{5,n-1}\dots x_{5,0}}_{n}\underbrace{x_{5,n-1}\dots x_{5,0}}_{n}$$

$$\underbrace{x_{5,n-1}\dots x_{5,0}}_{n}\underbrace{x_{5,n-1}\dots x_{5,0}}_{n}\underbrace{x_{5,n-1}\dots x_{5,0}}_{n}\underbrace{x_{5,n-1}\dots x_{5,3}}_{n-3} \tag{3.200}$$

$$a_2 = \overline{\underbrace{x_{1,2n-1}x_{1,2n-2}\dots x_{1,1}x_{1,0}}_{2n}}\,\overline{\underbrace{x_{2,4n}x_{2,4n-1}\dots x_{2,1}x_{2,0}}_{4n+1}}\,\underbrace{1\dots 11}_{2n-1} \tag{3.201}$$

$$a_3 = \underbrace{x_{2,2n}x_{2,n-1}\dots x_{2,0}}_{2n+1}\underbrace{0\dots 00}_{4n-1}\underbrace{x_{2,4n}x_{2,4n-1}\dots x_{2,n+2}}_{2n} \tag{3.202}$$

$$a_4 = \underbrace{0}_{1}\underbrace{x_{3,2n}x_{3,2n-1}\dots x_{3,1}x_{3,0}}_{2n+1}\underbrace{0\dots00}_{2n-1}\underbrace{x_{3,2n}x_{3,2n-1}\dots x_{3,1}x_{3,0}}_{2n+1}\underbrace{1\dots11}_{2n-2} \quad (3.203)$$

$$a_5 = \underbrace{\overline{x_{3,1}x_{3,0}}}_{2}\underbrace{1\dots11}_{2n-1}\underbrace{\overline{x_{3,2n}\dots x_{3,0}}}_{2n+1}\underbrace{1\dots11}_{2n-1}\underbrace{\overline{x_{3,2n}\dots x_{3,2}}}_{2n-1} \quad (3.204)$$

$$a_6 = \underbrace{11}_{2}\underbrace{\overline{x_{4,n}\dots x_{4,0}}}_{n+1}\underbrace{1\dots11}_{n-1}\underbrace{\overline{x_{4,n}\dots x_{4,0}}}_{n+1}\underbrace{1\dots11}_{n-1}\underbrace{\overline{x_{4,n}\dots x_{4,0}}}_{n+1}\underbrace{1\dots11}_{n-1}\underbrace{\overline{x_{4,n}\dots x_{4,0}}}_{n+1}\underbrace{1\dots11}_{n-3}$$

(3.205)

$$a_7 = \underbrace{x_{4,2}x_{4,1}x_{4,0}}_{3}\underbrace{0\dots00}_{n-1}\underbrace{x_{4,n}\dots x_{4,0}}_{n+1}\underbrace{0\dots00}_{n-1}\underbrace{x_{4,n}\dots x_{4,0}}_{n+1}\underbrace{0\dots00}_{n-1}\underbrace{x_{4,n}\dots x_{4,0}}_{n+1}\underbrace{0\dots00}_{n-1}\underbrace{x_{4,n}\dots x_{4,3}}_{n-2}$$

(3.206)

Also, since x_1 is a 2n-bit number, *X* in (3.198) can be obtained as

$$X = x_1 + 2^{2n}M = \underbrace{M_{8n-1}M_{8n-2}\dots M_1M_0}_{8n}\underbrace{x_{1,2n-1}x_{1,2n-2}\dots x_{1,1}x_{1,0}}_{2n} \quad (3.207)$$

Example: Consider the moduli set $\{2^{2n},\ 2^{4n}+1,\ 2^{2n}+1, 2^n+1,\ 2^n-1\}$ where n=3. The weighted number *X* can be calculated from its RNS representation (7, 3621, 32, 1, 3) as follows:

For n=3 the moduli set is {64, 4097, 65, 9, 7} and also residues have binary representation as below

$$x_1 = 7 = (000111)_2$$

$$x_2 = 3621 = (0111000100101)_2$$

$$x_3 = 32 = (0100000)_2$$

$$x_4 = 1 = (0001)_2$$

$$x_5 = 3 = (011)_2$$

According to (3.200), (3.201), (3.202), (3.203), (3.204), (3.205), (3.206) and (3.199) we have

$$a_1 = (011011011011011011011011)_2 = 7190235$$

$$a_2 = (111000100011101101011111)_2 = 14826335$$

$$a_3 = (010010100000000000011100)_2 = 4849692$$

$$a_4 = (001000000000001000000000)_2 = 2097664$$

$$a_5 = (111111101111111111110111)_2 = 16744439$$

$$a_6 = (111110111110111110111110)_2 = 16510910$$

$$a_7 = (001000001000001000001000)_2 = 2130440$$

$$M = |64349715|_{16777215} = (110101011110011000010110)_2 = 14018070$$

Substituting the value of *M* in (3.207), *X* can be calculated as below

$$X = (110101011110011000010110000111)_2 = 897156487$$

We can see that $|897156487|_{64} = 7$, $|897156487|_{4097} = 3621$, $|897156487|_{65} = 32$, $|897156487|_9 = 1$, $|897156487|_7 = 3$ and therefore the calculated *X* is indeed the weighted value of the residue representation (7, 3621, 32, 1, 3) with respect to the moduli set {64, 4097, 65, 9, 7}.

Hardware Implementation: The reverse converter hardware architecture for the five moduli set $\{2^{2n},\ 2^{4n}+1,\ 2^{2n}+1, 2^n+1,\ 2^n-1\}$ with corresponding residues $(x_1, x_2, x_3, x_4, x_5)$ of the integer *X* is shown in Fig. 3.8. Area and Delay specification for each part of the converter are shown in Table 3.8.

Table 3.8

Area and Delay Specifications of Reverse Converter for the moduli set S_6 using New CRT I

Parts	FA	NOT	XOR/AND pairs	XNOR/OR pairs	Delay
OPU1		9n+3			t_{NOT}
CSA1	2n+2		4n-1	2n-1	t_{FA}
CSA2	4		2n-2	6n-2	t_{FA}
CSA3	4n+2		4n-2		t_{FA}
CSA4	8n				t_{FA}
CSA5	8n				t_{FA}
CPA1	8n				$16n\ t_{FA}$
Total Area	(30n+8)A_{FA}+ (9n+3)A_{NOT}+ (10n-5)A_{XOR}+ (10n-5)A_{AND}+ (8n-3)A_{XNOR}+ (8n-3)A_{OR}				
Total Delay	(16n+4)t_{FA} + t_{NOT}				

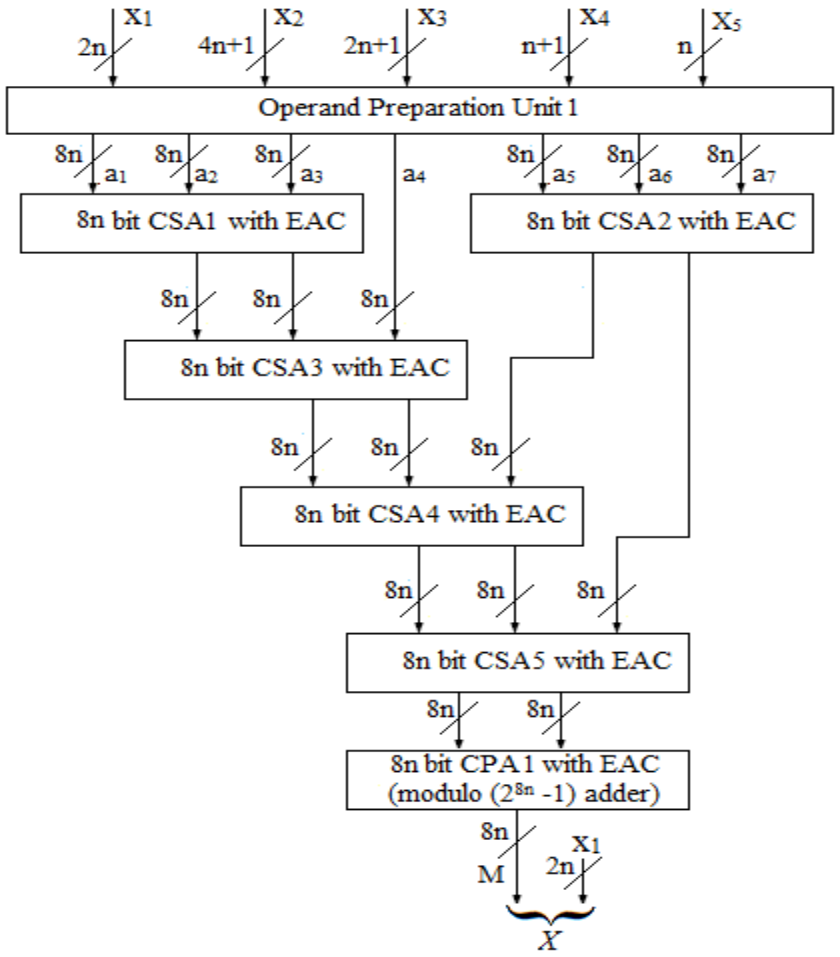


Figure 3.8 Reverse Converter for the moduli set S_6 using New CRT I

4. EVALUATION AND COMPARISON

4.1 Area and Delay Comparisons for Four Moduli Set Reverse Converters:

In this Section, the hardware cost and delays of the reverse converters discussed in Section 2 are compared. The comparison is done by adopting a common practice to flatten the architecture to allow an estimation of the area and delay complexities in terms of units of 1-bit Full Adders (area and delay of inverters and multiplexers are not considered in order to simplify comparisons). The comparisons of area, delay, approximate dynamic range (DR) of reverse converters for the four moduli sets P_1', P_1 and P_2 are shown in Table 4.1. It is clear that the converter for moduli set P_1' designed using New CRT I and MRC [19] is faster than other reverse converters. Also, this converter has low hardware cost when compared to other converters for a given dynamic range.

Table 4.1

Comparisons of reverse converters for four moduli sets P_1', P_1 and P_2

Moduli Sets		P_1'			P_1		P_2	
Conversion Algorithms		New CRT II	CRT and MRC	New CRT I + MRC[19]	New CRT II	CRT and MRC	New CRT II	CRT and MRC
n=4 (=3)*	**DR(≈)**	**15-bit**			15-bit		12-bit	
	Area (A_{FA})	53	57	**45**	71	72	67	76
	Delay (t_{FA})	53	61	**39**	49	55	46	52
n=6 (=5)*	**DR(≈)**	**23-bit**			23-bit		20-bit	
	Area (A_{FA})	105	111	**76**	135	136	133	148
	Delay (t_{FA})	81	93	**66**	79	89	76	86
n=8 (=7)*	**DR(≈)**	**31-bit**			31-bit		28-bit	
	Area (A_{FA})	173	181	**111**	215	216	215	236
	Delay (t_{FA})	140	124	**89**	107	122	105	119
n=10 (=9)*	**DR(≈)**	**39-bit**			39-bit		36-bit	
	Area (A_{FA})	257	267	**150**	311	312	313	340
	Delay (t_{FA})	134	154	**111**	136	154	160	151

The '*' indicates the odd value of n is for the moduli set P_2.

4.2 Area and Delay Comparisons for Five Moduli Set Reverse Converters:

The comparisons of area, delay, approximate dynamic range (DR) of reverse converters for the five moduli sets S_1, S_2, S_3, S_4, S_5 and S_6 are shown in Table 4.2. It is clear that the converter for moduli set S_6 designed using New CRT I is not only faster than other reverse converters but also has low hardware cost. The converter for moduli set S_6 is the best suitable converters when a dynamic range between 20 to 100-bits is desired. For a dynamic range less than 16-bits the converter for moduli set S_4 designed using New CRT I and MRC (Method 1) is recommended. Also, other converters can be selected from Table 4.2 for a given dynamic range considering the area and delay factors.

4.3 Choice of Reverse Converters:

The reverse converter for four moduli set P_1' is best suitable for a dynamic range less than 20- bits as it has less area and delay when compared to reverse converters of five moduli sets. If a high speed converter is required for a dynamic range between 20 to 40-bits, then the reverse converter for five moduli set S_6 is recommended over reverse converter for P_1'. If a low cost converter is required for a dynamic range between 20 to 40-bits, then the reverse converter for four moduli set P_1' is suggested over reverse converter for S_6. For a dynamic range greater than 40- bits the reverse converter for five moduli set S_6 is desirable.

Table 4.2

Comparisons of reverse converters for five moduli sets S_1, S_2, S_3, S_4, S_5 and S_6

Moduli Sets		S_1	S_2	S_3		S_4		S_5	S_6
Conversion Algorithms		New CRT I + MRC	New CRT I + MRC	New CRT I + MRC Method 1	New CRT I + MRC Method 2	New CRT I + MRC Method 1	New CRT I + MRC Method 2	New CRT I	New CRT I
n=2	**DR(≈)**	-	-	13-bit		**15-bit**		-	**20-bit**
	Area (A_{FA})	-	-	55	62	**58**	61	-	**96**
	Delay (t_{FA})	-	-	44	55	**45**	55	-	**32**
n=3	**DR(≈)**	-	-	20-bit		**23-bit**		27-bit	**30-bit**
	Area (A_{FA})	-	-	90	118	**95**	117	144	**144**
	Delay (t_{FA})	-	-	67	83	**68**	83	52	**52**
n=4	**DR(≈)**	25-bit	22-bit	**27-bit**		**31-bit**		36-bit	**40-bit**
	Area (A_{FA})	154	129	**129**	190	**136**	189	192	**192**
	Delay (t_{FA})	92	121	**90**	110	**91**	110	68	**68**
n=5	**DR(≈)**	-	-	34-bit		39-bit		45-bit	**50-bit**
	Area (A_{FA})	-	-	172	278	181	277	240	**240**
	Delay (t_{FA})	-	-	113	136	114	136	84	**84**
n=6	**DR(≈)**	39-bit	34-bit	41-bit		47-bit		54-bit	**60-bit**
	Area (A_{FA})	332	202	219	382	230	381	288	**288**
	Delay (t_{FA})	147	186	135	163	136	163	100	**100**
n=7	**DR(≈)**	-	-	48-bit		55-bit		63-bit	**70-bit**
	Area (A_{FA})	-	-	270	502	283	501	336	**336**
	Delay (t_{FA})	-	-	160	189	159	189	116	**116**
n=8	**DR(≈)**	53-bit	46-bit	55-bit		63-bit		72-bit	**80-bit**
	Area (A_{FA})	574	279	325	638	340	637	384	**384**
	Delay (t_{FA})	202	251	180	216	181	216	132	**132**
n=9	**DR(≈)**	-	-	62-bit		71-bit		81-bit	**90-bit**
	Area (A_{FA})	-	-	384	790	401	789	432	**432**
	Delay (t_{FA})	-	-	202	242	203	242	148	**148**
n=10	**DR(≈)**	67-bit	58-bit	69-bit		79-bit		90-bit	**100-bit**
	Area (A_{FA})	880	360	447	958	466	957	480	**480**
	Delay (t_{FA})	257	315	225	268	226	268	164	**164**

5. CONCLUSION AND FUTURE WORK

This research is mainly focused on designing reverse conversion architectures for the four and five moduli sets proposed in [18] for binary domain. The five moduli sets proposed in [18] are modified and six new five moduli sets have been proposed in this research. The proposed reverse conversion techniques are based on Traditional Chinese Remainder Theorem, Mixed Radix Conversion and New Chinese Remainder Theorems (New CRT I and New CRT II). The various architectures, for these moduli sets, are all based on Full Adders, thereby providing simple design and VLSI efficient implementation of adder based architectures. The reverse converters hardware and delay specifications are analyzed and a suitable converter has been suggested for a given dynamic range. The overall dynamic range supported by the reverse converters is from as small as 12-bits up to 100-bits.

The future work that can be derived out of this research is designing reverse converters for six, seven and larger moduli sets proposed in [18] or extending the new five moduli sets proposed in this research to six, seven and larger moduli sets, so that the reverse converters for the large moduli sets further increases the parallelism and reduces the size of each residue channel for a given dynamic range.

REFERENCES

[1] Szabo, N.S., and Tanaka, R.I.: "Residue arithmetic and its applications to computer technology" (McGraw Hill Press, New York, 1967)

[2] M. A. Soderstrand, W. K. Jenkins, G. A. Jullien, and F. J. Taylor, Eds., "*Residue Number System Arithmetic: Modern Applications in Digital Signal Processing*," New York: IEEE Press, 1986.

[3] W. K. Jenkins and B. J. Leon, "The use of residue number systems in the design of finite impulse response digital filters," *IEEE Trans. Circuits Syst.*, vol. CAS-24, no. 4, pp. 191–201, Apr. 1977.

[4] M. A. Soderstrand, "A high-speed low-cost recursive digital filter using residue number arithmetic," *Proc. IEEE*, vol. 65, pp. 1065–1067, Jul. 1977.

[5] H. K. Nagpal, G. A. Jullien, and W. C. Miller, "Processor architectures for two-dimensional convolvers using a single multiplexed computational element with finite field arithmetic," *IEEE Trans. Comp.*, vol. C-32, no. 11, pp. 989–1000, Nov. 1983.

[6] F. J. Taylor, G. Papadourakis, A. Skavantzos, and A. Stouraitis, "A radix-4 FFT using complex RNS arithmetic," *IEEE Trans. Comp.*, vol. C-34, no. 6, pp. 573–576, Jun. 1985.

[7] W. A. Chren, "RNS-based enhancements for direct digital frequency synthesis," IEEE Trans. Circuits Syst. I, Fundam. Theory Appl.I, Anlaog Digit. Signal Process., Anlaog Digit. Signal Process., vol. 42, no. 8, pp. 516–524, Aug. 1995.

[8] W. Wang, M. N. S. Swamy, and M. O. Ahmad, "RNS application for digital image processing," in Proc. 4th IEEE Int. Workshop System-on- Chip for Real Time Appl., 2004, pp. 77–80.

[9] V. T. Goh and M. U. Siddiqi, "Multiple error detection and correction based on redundant residue number systems," IEEE Trans. Commun., vol. 56, no. 3, pp. 325–330, Mar. 2008.

[10] S. Timarchi and K. Navi, "Efficient class of redundant residue number system," in Proc. IEEE Int. Symp. Intell. Signal Process., 2007, pp. 1–6.

[11] Yuke Wang, "Residue-to-Binary Converters Based On New Chinese Remainder Theorems," *IEEE Transactions on Circuits and Systems – II: Analog and Digital Signal Processing*, vol. 47, No. 3, pp.197–205, March 2000.

[12] Y. Wang, "New Chinese Remainder Theorems," in Proceedings of the Thirty Second Asilomar Conference on Signals, Systems and Computers, vol. 1, pp. 165-171, Nov. 1998.

[13] Wang, Y., Song, X., Aboulhamid, M., Shen, H., "Adder based residue to binary number converters for (2^n-1, 2^n, 2^n+1)," *IEEE Transactions on Signal Processing*, vol.50, no.7, pp.1772-1779, Jul 2002.

[14] A.S. Molahosseini, K. Navi, C. Dadkhah, O. Kavehei, S. Timarchi, "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 Trans. Circuits and Systems-I*, vol. 57, no. 4, pp. 823-835, 2010.

[15] S. J. Piestrak, "A high speed realization of a residue to binary converter," *IEEE Trans. Circuits Syst. II, Analog. Digit. Signal Process.*, vol. 42, no. 10, pp. 661–663, Oct. 1995.

[16] S. J. Piestrak, "Design of residue generators and multioperand modular adders using carry-save adders," *IEEE Trans. Comput.*, vol. 423, no. 1, pp. 68–77, Jan. 1994.

[17] Hwang, K.: 'Computer arithmetic: principle, architecture and design' (Wiley Press, New York, 1979)

[18] Mohammad Abdallah and Alexander Skavantzos, "On MultiModuli Residue Number Systems with Moduli of Forms r^a, r^b - 1, r^c + 1," *IEEE Transactions On Circuits and Systems – I*: Regular Papers, vol. 52, No. 7, July 2005.

[19] B. Cao, T. Srikanthan, and C. H. Chang, "Efficient reverse converters for the 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}," *Proc. IEE Comput. Digit. Tech.*, vol. 152, no. 5, pp. 687–696, Sep. 2005.

[20] Cao, B., Chang, C.-H., Srikanthan, T., "A Residue-to-Binary Converter for a New Five-Moduli Set," Circuits and Systems I: *IEEE Transactions on Regular Paper*, vol.54, no.5, pp.1041-1049, May 2007.

[21] Cao, B., Chang, C.-H., Srikanthan, T., "Adder based residue to binary converters for a new balanced 4-moduli set," Image and Signal Processing and Analysis, 2003. ISPA 2003. Proceedings of the 3rd International Symposium, vol.2, no., pp. 820- 825 Vol.2, 18-20 Sept. 2003.

[22] Reto Zimmermann "Lecture notes on Computer Arithmetic: Principles, Architectures and VLSI Design," Integrated System Laboratory, Swiss Federal Institute of Technology (ETH) Zurich, Mar, 16, 1999. URL http://www.iis.ee.ethz.ch/~zimmi/publications/comp_arith_notes.pdf.

[23] Narendran Narayanaswamy, Alex Skavantzos, Thanos Stouraitis, "Optimal Modulus Sets for Efficient Residue-to-Binary Conversion Using the New Chinese Remainder Theorems" *In Proceedings of the 17th IEEE International Conference on Electronics, Circuits, and Systems*, Athens, December 2010.

[24] Skavantzos, A., *Dr. Alexander Skavantzos: Home Page*. Retrieved January 30, 2012, from LSU Electrical and Computer Engineering: http://www.ece.lsu.edu/alex/index.html

APPENDIX A

MULTIPLICATIVE INVERSE MODULO CALCULATION

The multiplicative inverse of a number *a* modulo *b* is denoted as a^{-1}*modulo b*. The value a^{-1}*modulo b* exists if and only if *a* and *b* are co-prime to each other, that is, greatest common divisor of *a* and *b* is 1.

$$|a^{-1}|_m = b\ ;\ b\ \in \{1, 2, \dots, m-1\} \tag{A.1}$$

where b is such that $|\ a \cdot b\ |_m = 1$

Example: $|5^{-1}|_{11} = 9$

There are many theorems to calculate multiplicative inverse modulus values, and some familiar ones are Euclidean algorithm, Euler Totient function, Euler and Fermat's theorems. The following method based on Extended Euclidean algorithm is discussed here which is useful in calculating multiplicative inverse modulo.

A.1 Extended Euclidean Algorithm

Extended Euclidean algorithm is the extension of Euclidean algorithm, which is mainly used when two numbers *a* and *b* are co-prime to each other. It states that,

$$ax + by = gcd\ (a, b) \tag{A.2}$$

where a, b are integers.

By the definition of inverse modulus, *ax* is congruent to *(1 mod b)*

Hence, *b* is the divisor of *ax – 1*, and it gives the following,

$$ax - by = 1 \tag{A.3}$$

In the above equation, *a* and *b* are the numbers whose inverse modulo value is to be found out, *x* is the inverse modulus value and *y* is an integer and it can be ignored.

Example: Find the value of 13^{-1} mod 7.

Using the equation (A.3), and approaching trial and error method, it is found out that x =6 and y = 11. Ignoring the value of y, the value of 13^{-1} mod 7 is 6.

A.2 Code in C to Calculate Multiplicative Inverse:

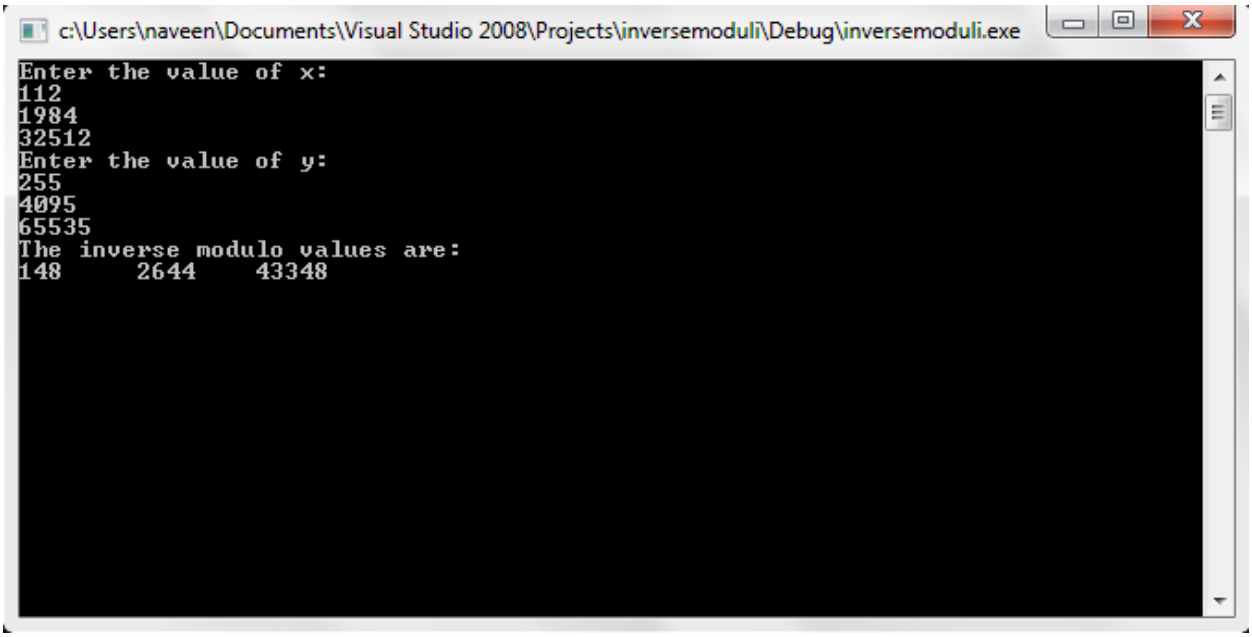
The following code in C is used to simulate the series of multiplicative inverse values, and is based on Extended Euclidean algorithm.

Code:

```
/* To calculate multiplicative inverse series */
#include<stdio.h>
main(){
    long long int x[10], y[10],j;
    printf("Enter the value of x:\n");
    for(j=0;j<3;j++){
        scanf("%lld",&x[j]);
    }
    printf("Enter the value of y:\n");
    for(j=0;j<3;j++){
        scanf("%lld",&y[j]);
    }
    printf("The inverse modulo values are:\n");
    Inverse(x,y);
        getch();
}
```

```
int Inverse(long long int a[], long long int n[]){
    long long int k, i[3], v[3], d[3], t[3], x[3];
        for(k=0;k<3;k++){
            i[k] = n[k], v[k] = 0, d[k] = 1;
            while (a[k]>0){
              t[k] = i[k]/a[k], x[k] = a[k];
              a[k] = i[k] % x[k];
              i[k] = x[k];
              x[k] = d[k];
              d[k] = v[k] - t[k]*x[k];
              v[k] = x[k];
            }
            v[k] %= n[k];
            if (v[k]<0) v[k] = (v[k]+n[k])%n[k];
                  printf("%lld \t",v[k]);
        }
        printf("\n\n");
    }
```

Result:


c:\Users\naveen\Documents\Visual Studio 2008\Projects\inversemoduli\Debug\inversemoduli.exe
Enter the value of x:
112
1984
32512
Enter the value of y:
255
4095
65535
The inverse modulo values are:
148 2644 43348

APPENDIX B

PROOFS FOR THE SETS TO BE PAIRWISE RELATIVELY PRIME

B.1 The Set $S_1 = \{2^{2n-2}+1, 2^{n-1}-1, 2^{n-1}+1, 2^n, 2^{2n}+1\}$, where $n = 2k, k = 2, 3, 4, \ldots$ Is Pairwise Relatively Prime

Proof:

The proof for the moduli $2^{n-1}-1, 2^{n-1}+1, 2^n$ to be pairwise relatively prime is given in [18] for moduli set P_1 for binary radix. Therefore, we shall prove that the moduli $2^{2n-2}+1$, $2^{2n}+1$ are pairwise relatively prime to each other and also pairwise relatively prime to the moduli $2^{n-1}-1, 2^{n-1}+1, 2^n$.

Let a/b mean "a divides b."

It is true that, if a/b and a/c, then $a/[k_1 b \pm k_2 c]$. Let d be a common divisor of $2^{2n-2}+1$ and $2^{2n}+1$. Then $d/2^{2n-2}+1$ and $d/2^{2n}+1$ implies $d/[2^2(2^{2n-2}+1) - 2^{2n}+1]$ and in turn implies $d/3$ or d= 1, 3. But 3 does not divide either $2^{2n-2}+1$ or $2^{2n}+1$ for even values of n. Therefore d=1. Thus the only common divisor of $2^{2n-2}+1$ and $2^{2n}+1$ is 1 and therefore $2^{2n-2}+1$ and $2^{2n}+1$ are relatively prime.

Finding gcd$(2^{2n-2}+1, 2^{n-1}-1)$ using Euclidean algorithm:

$|2^{2n-2}+1|_{2^{n-1}-1} = 2$

$|2^{n-1}-1|_2 = 1$

$|2|_1 = 0$

Therefore, gcd$(2^{2n-2}+1, 2^{n-1}-1)$=1

Finding gcd$(2^{2n-2}+1, 2^{n-1}+1)$ using Euclidean algorithm:

$|2^{2n-2}+1|_{2^{n-1}+1} = |2^{n-1}(2^{n-1}+1) - 2^{n-1}+1|_{2^{n-1}+1} = |2^{n-1}(0) - 2^{n-1}+1|_{2^{n-1}+1} = 2$

$|2^{n-1}+1|_2 = 1$

$|2|_1 = 0$

Therefore, gcd($2^{2n-2}+1, 2^{n-1}+1$) =1

Finding gcd($2^{2n-2}+1, 2^n$) using Euclidean algorithm:

$|2^{2n-2}+1|_{2^n} = |0+1|_{2^n} = 1$

$|2^n|_1 = 0$

Therefore, gcd($2^{2n-2}+1, 2^n$) =1

Finding gcd($2^{2n}+1, 2^{n-1}-1$) using Euclidean algorithm:

$|2^{2n}+1|_{2^{n-1}-1} = |4 \cdot (2^{n-1} \cdot 2^{n-1}) + 1|_{2^{n-1}-1} = 5$

$$|2^{n-1}-1|_5 = \begin{cases} 2 & if\ n = 2k, k = 2, 4, 6 \ldots \\ 1 & if\ n = 2k, k = 3, 5, 7 \ldots \end{cases}$$

$|5|_2 = 1$ and $|2|_1 = 0$, also $|5|_1 = 0$

Therefore, gcd($2^{2n}+1, 2^{n-1}-1$)=1 for all even values of n greater than 2.

Finding gcd($2^{2n}+1, 2^{n-1}+1$) using Euclidean algorithm:

$|2^{2n}+1|_{2^{n-1}+1} = |4 \cdot (2^{n-1} \cdot 2^{n-1}) + 1|_{2^{n-1}+1} = 5$

$$|2^{n-1}+1|_5 = \begin{cases} 4 & if\ n = 2k, k = 2, 4, 6 \ldots \\ 3 & if\ n = 2k, k = 3, 5, 7 \ldots \end{cases}$$

$|5|_4 = 1$ and $|4|_1 = 0$, also $|5|_3 = 2$, $|3|_2 = 0$, $|2|_1 = 0$

Therefore, gcd($2^{2n}+1, 2^{n-1}+1$) =1 for all even values of n greater than 2.

Finding gcd($2^{2n}+1, 2^n$) using Euclidean algorithm:

$|2^{2n}+1|_{2^n} = |0+1|_{2^n} = 1$

$|2^n|_1 = 0$

Therefore, gcd($2^{2n}+1, 2^n$) =1

Since the greatest common divisors are one, the moduli set $S_1 = \{2^{2n-2}+1, 2^{n-1}-1, 2^{n-1}+1, 2^n, 2^{2n}+1\}$ is a co-prime set for all even values of n greater than 2.

B.2 The Set $S_2 = \{2^{2n-1}-1, 2^{n-1}-1, 2^n-1, 2^n, 2^n+1\}$, where $n = 2k, k = 2, 3, 4, \ldots$ Is Pairwise Relatively Prime

Proof:

The proof for the moduli $2^{n-1}-1, 2^n-1, 2^n, 2^n+1$ to be pairwise relatively prime is given in [18] for moduli set P_1' for binary radix. Therefore, we shall prove that the moduli $2^{2n-1}-1$ is pairwise relatively prime to the moduli $2^{n-1}-1, 2^n-1, 2^n, 2^n+1$.

Finding gcd($2^{2n-1}-1, 2^{n-1}-1$) using Euclidean algorithm:

$|2^{2n-1}-1|_{2^{n-1}-1} = |2\cdot 2^{n-1}\cdot 2^{n-1}-1|_{2^{n-1}-1} = 1$

$|2^{n-1}-1|_1 = 0$

Therefore, gcd($2^{2n-1}-1, 2^{n-1}-1$)=1

Finding gcd($2^{2n-1}-1, 2^n-1$) using Euclidean algorithm:

$|2^{2n-1}-1|_{2^n-1} = |2^n(2^{n-1})-1|_{2^n-1} = 2^{n-1}-1$

$|2^n-1|_{2^{n-1}-1} = |2\cdot 2^{n-1}-1|_{2^{n-1}-1} = 1$

$|2^{n-1}-1|_1 = 0$

Therefore, gcd($2^{2n-1}-1, 2^n-1$) =1

Finding gcd($2^{2n-1}-1, 2^n+1$) using Euclidean algorithm:

$|2^{2n-1}-1|_{2^n+1} = |2^n(2^{n-1})-1|_{2^n+1} = |-1\,(2^{n-1})-1|_{2^n+1} = 2^{n-1}$

$|2^n+1|_{2^{n-1}} = |2\cdot 2^{n-1}+1|_{2^{n-1}} = 1$

$|2^{n-1}|_1 = 0$

Therefore, gcd($2^{2n-1}-1, 2^n+1$) =1

Finding gcd($2^{2n-1}-1, 2^n$) using Euclidean algorithm:

$|2^{2n-1}-1|_{2^n}$= $|0-1|_{2^n}$= $|2^n-1|_{2^n}$=2^n-1

$|2^n|_{2^n-1}$= 1

$|2^n-1|_1$= 0

Therefore, gcd($2^{2n-1}-1, 2^n$) =1

Since the greatest common divisors are one, the moduli set $S_2 = \{2^{2n-1}-1, 2^{n-1}-1, 2^n-1, 2^n, 2^n+1\}$ is pairwise co-prime for all even values of n greater than 2.

B.3 The Set $S_3 = \{2^{2n-1}-1, 2^{2n}+1, 2^n-1, 2^n, 2^n+1\}$, where $n = 2, 3, 4, \ldots$ Is Pairwise Relatively Prime

Proof:

It is well known that the prominent moduli $2^n-1, 2^n, 2^n+1$ are pairwise relatively prime to each other. The proof for the moduli $2^{2n}+1$ to be pairwise relatively prime to the moduli $2^n-1, 2^n, 2^n+1$ is given in [14]. Also, the proof for the moduli $2^{2n-1}-1$ to be pairwise relatively prime to the moduli $2^n-1, 2^n, 2^n+1$ is given in Appendix B (Section B.2). Therefore, we shall prove that the moduli $2^{2n-1}-1$ is pairwise relatively prime to the moduli $2^{2n}+1$.

Let a/b mean "a divides b."

It is true that, if a/b and a/c, then $a/[k_1 b \pm k_2 c]$. Let d be a common divisor of $2^{2n-1}-1$ and $2^{2n}+1$. Then $d/2^{2n-1}-1$ and $d/2^{2n}+1$ implies $d/[-2(2^{2n-1}-1)+(2^{2n}+1)]$ and in turn implies $d/3$ or d= 1, 3. But 3 does not divide either $2^{2n-1}-1$ or $2^{2n}+1$ for all values of n greater than 1. Therefore d=1. Thus the only common divisor of $2^{2n-1}-1$ and $2^{2n}+1$ is 1 and therefore $2^{2n-1}-1$ and $2^{2n}+1$ are relatively prime.

Therefore the moduli set $S_3 = \{2^{2n-1} - 1, 2^{2n} + 1, 2^n - 1, 2^n, 2^n + 1\}$ is pairwise co-prime for all values of n greater than 1.

B.4 The Set $S_4 = \{2^{2n-1} - 1, 2^{2n} + 1, 2^n - 1, 2^{2n}, 2^n + 1\}$, where $n = 2, 3, 4, \ldots$ Is Pairwise Relatively Prime

Proof:

The proof for the moduli $2^{2n} + 1, 2^n - 1, 2^{2n}, 2^n + 1$ to be pairwise relatively prime is given in [14], and the proof for the moduli $2^{2n-1} - 1, 2^{2n} + 1, 2^n - 1, 2^n + 1$ to be pairwise relatively prime is given in Appendix B (Section B.3). Therefore, we shall prove that the moduli $2^{2n-1} - 1$ is pairwise relatively prime to the moduli 2^{2n}.

Finding gcd($2^{2n-1} - 1, 2^{2n}$) using Euclidean algorithm:

$|2^{2n-1} - 1|_{2^{2n}} = 2^{2n-1} - 1$

$|2^{2n}|_{2^{2n-1}-1} = |2 \cdot 2^{2n-1}|_{2^{2n-1}-1} = 2$

$|2^{2n} - 1|_2 = 1$

$|2|_1 = 0$

Therefore, gcd($2^{2n-1} - 1, 2^{2n}$) =1

Since the greatest common divisor is one, the moduli set $S_4 = \{2^{2n-1} - 1, 2^{2n} + 1, 2^n - 1, 2^{2n}, 2^n + 1\}$ is pairwise co-prime for all values of n greater than 1.

B.5 The Set $S_5 = \{2^{4n} + 1, 2^{2n} + 1, 2^n - 1, 2^n, 2^n + 1\}$, where $n = 3, 4, 5 \ldots$ Is Pairwise Relatively Prime

Proof:

The proof for the moduli $2^{2n} + 1, 2^n - 1, 2^n, 2^n + 1$ to be pairwise relatively prime is given in Appendix B (Section B.4). Therefore, we shall prove that the moduli $2^{4n} + 1$ is pairwise relatively prime to the moduli $2^{2n} + 1, 2^n - 1, 2^n + 1, 2^n$.

Finding gcd($2^{4n}+1, 2^{2n}+1$) using Euclidean algorithm:

$|2^{4n}+1|_{2^{2n}+1}$= 2

$|2^{2n}+1|_{2}$= 1

$|2|_{1}$= 0

Therefore, gcd($2^{4n}+1, 2^{2n}+1$)=1

Finding gcd($2^{4n}+1, 2^{n}-1$) using Euclidean algorithm:

$|2^{4n}+1|_{2^{n}-1}$= 2

$|2^{n}-1|_{2}$= 1

$|2|_{1}$= 0

Therefore, gcd($2^{4n}+1, 2^{n}-1$)=1

Finding gcd($2^{4n}+1, 2^{n}+1$) using Euclidean algorithm:

$|2^{4n}+1|_{2^{n}+1}$= 2

$|2^{n}+1|_{2}$= 1

$|2|_{1}$= 0

Therefore, gcd($2^{4n}+1, 2^{n}+1$)=1

Finding gcd($2^{4n}+1, 2^{n}$) using Euclidean algorithm:

$|2^{4n}+1|_{2^{n}}$= $|0+1|_{2^{n}}$= 1

$|2^{n}|_{1}$= 0

Therefore, gcd($2^{4n}+1, 2^{n}$) =1

Since the greatest common divisors are one, the moduli set $S_5 = \{2^{4n}+1, 2^{2n}+1, 2^{n}-1, 2^{n}, 2^{n}+1\}$ is pairwise co-prime for all values of n greater than 2.

B.6 The Set $S_6 = \{2^{4n}+1, 2^{2n}+1, 2^n-1, 2^{2n}, 2^n+1\}$, where $n = 2, 3, 4 \ldots$ Is Pairwise Relatively Prime

Proof:

The proof for the moduli $2^{4n}+1, 2^{2n}+1, 2^n-1, 2^n+1$ to be pairwise relatively prime is given in Appendix B (Section B.5). Therefore, we shall prove that the moduli$2^{4n}+1$ is pairwise relatively prime to the moduli 2^{2n}.

Finding gcd($2^{4n}+1, 2^{2n}$) using Euclidean algorithm:

$|2^{4n}+1|_{2^{2n}} = |0+1|_{2^{2n}} = 1$

$|2^{2n}|_1 = 0$

Therefore, gcd($2^{4n}+1, 2^{2n}$) =1

Since the greatest common divisor is one, the moduli set $S_6 = \{2^{4n}+1, 2^{2n}+1, 2^n-1, 2^{2n}, 2^n+1\}$ is pairwise co-prime for all values of n greater than 1.

VITA

Naveen Kumar Samala was born in Hyderabad, capital city of the state of Andhra Pradesh, India. His father is a chauffeur and his mother is a draper. He has two siblings, one elder sister who is a Teacher at a Secondary School and one younger brother who is doing business in drapery. He received his Bachelor of Engineering in Electrical and Electronic Engineering degree with distinction from Osmania University, Andhra Pradesh, India. Upon graduation, he joined Infosys Technologies Limited, Karnataka, India, as a Systems Engineer and worked there for about two years on JAVA technology and in Banking Domain. Later, he enrolled in Louisiana State University, to pursue a master's degree in the Department of Electrical and Computer Engineering with computers as major area. His areas of interests are web designing, software application development and database management. He was also employed as Student Worker/Computer Programmer to work on High Performance Computing Linux clusters in Agricultural Department, Louisiana State University. With his expertise in coding C++ programs and creating Dynamic Linked Libraries, he collaborated with one of the professors in Chemical Engineering Department, Louisiana State University. Presently, he is employed as Graduate Assistant/System Administrator in the College of Humanities and Social Sciences, Louisiana State University. He will be graduating with the degree of Master of Science in Electrical Engineering in May 2012.