Volume 2, Issue 8, August 2012 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

www.ijarcsse.com

Research Paper

Available online at: www.ijarcsse.com

An Efficient Reverse Converter for the New Modulus Set $\{2^{2n+2}-1,\ 2^{2n+1}-1,\ 2^{n}\}$

Samira Modiri[*]
Department of Computer Engineering
Dezful Branch, Islamic Azad University
Dezful, Iran

Ali Movaghar
Department of Computer Engineering
Sharif University of Technology
Tehran, Iran

Ali Barati
Department of Computer Engineering
Dezful Branch, Islamic Azad University
Dezful, Iran

Abstract*— As two critical issues in residue number systems are modulus set selection and efficient design of a reverse converter, a new residue number system modulus set $\{2^{2n+2}-1,\ 2^{2n+1}-1,\ 2^{n}\}$ is introduced in this paper and a high performance residue to binary converter is designed based on mixed radix conversion algorithm and the purposed modulus set. Comparison with the other reverse converters found in the literatures based on (5n) and (4n)-bit dynamic range modulus sets shows the proposed reverse converter design improves the conversion delay and results in hardware saving.

***Keywords*— residue number system, reverse converter, mixed radix conversion**

I. Introduction

Residue number system (RNS) is a carry-free number system, which has been used for achieving high-performance computing system [1] and has many applications in today's world such as image processing systems[2], RSA algorithm [3], digital communications [4], video filtering [5], Elliptic curve cryptography [6], M-ary Orthogonal keyed communication scheme [7], and general purpose RISC DSP [8].

In residue number systems, each number is broken and a set of remainders based on the modulus set is constructed. The operations are performed on the remainders paralleled, instead of a number itself. Thus the hardware requirement is reduced and speed of operations is improved. Because the operations are performed on the smaller unit processing, and all of the tasks are performed parallel. Moreover, the modulus in the modulus set act as secret keys, because for convert back the received remainders to the original number need to know the modulus set. Therefore, data transmission is secure in residue number systems, and if an adversary can acquire the sent message, he can not decrypt the packet without having the modulus in the modulus set. Two critical issues in residue number systems are modulus set selection and design and implementation of an efficient reverse converter. Finding an appropriate modulus set is difficult, because the modules must chosen as we can find closed-form multiplicative inverses for them to have a good design for the reverse converter. Multiplicative inverse is a natural number that can be defined as flows: multiplicative inverse of modulo m_i based on modulo m_j is equal to k, if $|k \times m_i|_{m_j} = 1$.

Another definition in residue number systems is dynamic range that is equal to product of all modulus in the modulus set, and denotes the interval of integers that can be represented uniquely in residue number system representation [9]. Moreover, there are two basic algorithms for designing the residue to binary converter, called Chinese remainder theorem (CRT) [10] and mixed radix conversion (MRC) [11]. Mixed radix conversion algorithm is sequential and suitable for design the reverse converters for the modulus set with three modulus. Up to now, many modulus set were presented and efficient reverse converters were designed for them. Famous modulus set is $\{2^n-1, 2^n, 2^n+1\}$ and many different reverse converters were designed for it [12-14]. Dynamic range for this modulus set is equal to (3n)-bits. For applications that need to higher dynamic range, the modulus set $\{2^n-1, 2^n, 2^n+1\}$ is not suitable. Therefore, other modulus sets with (4n), (5n), and (6n)-bits dynamic range were presented. For example, $\{2^n-1, 2^n, 2^n+1, 2^{n+1}+1\}$ [15, 16] and $\{2^n, 2^{2n}-1, 2^{2n}+1\}$ [17] has 4n-bit and 5n-bit dynamic range, respectively.In this paper, a new 3-modulus set $\{2^{2n+2}-1,\ 2^{2n+1}-1,\ 2^{n}\}$with (5n)-bits dynamic range is proposed and a high speed and low complex reverse converter is designed based on MRC algorithm.The rest of the paper is organized as follows: An efficient reverse converter based on the new proposed 3-main modulus set $\{2^{2n+2}-1,\ 2^{2n+1}-1,\ 2^{n}\}$ is designed and implemented in section II. In section III, performance of the proposed reverse converter is evaluated in terms of speed of operations and hardware requirement. Finally, the paper is concluded in section IV.

II. Design and Implementation of the Proposed Reverse Converter

A residue number system is defined in terms of relatively prime modulus set $\{P_1,\ P_2, \dots, P_n\}$ that is $\gcd(P_i, P_j) = 1$ for $(i \neq j)$. A weighted number X can be represented as $X = (x_1 x_2 \dots x_n)$, where

$$x_i = X \bmod P_i = |X|_{P_i}, \; 0 \le x_i < \mathrm{P_i} \tag{1}$$

Such a representation is unique for any integer X in the range $[0, M)$where $M = P_1 \, P_2 \dots P_n$is the dynamic range of the moduli set $\{P_1 \, P_2 \dots P_n\}$ [18]. The residue to binary conversion can be performed using the MRC as follows:

$$X = V_n \prod_{i=1}^{n} P_i + \cdots + V_3 P_2 P_1 + V_2 P_1 + V_1 \tag{2}$$

The coefficients $\mathrm{V_i}P$ can be obtained from residues by:

$$V_1 = \mathrm{x}_1 \tag{3}$$

$$V_2 = \left|(x_2 - x_1)\, |P_1^{-1}|_{P_2}\right|_{P_2} \tag{4}$$

$$V_3 = \left|((x_3 - x_1)|P_1^{-1}|_{P_3} - V_2)\, |P_2^{-1}|_{P_3}\right|_{\mathrm{P}_3} \tag{5}$$

In the general case, we have

$$V_n = (((\mathrm{x_n} - V_1)\, |P_1^{-1}|_{P_n} - V_2)\, |P_2^{-1}|_{P_n} - \quad \dots - V_{n-1})\, |P_{n-1}^{-1}|P_n \,|_{P_n} \tag{6}$$

Where $|P_i^{-1}|_{P_j}$ is the multiplicative inverse of $\mathrm{P_i}$ modulo $\mathrm{P_j}$. The modular multiplicative inverse of moduli m can be found using the extended Euclidean algorithm.

According to the Equations 2 to 5, we can design the proposed reverse converter for the new 3-moduli set $\{2^{2n+2} - 1,\ 2^{2n+1} - 1,\ 2^n\}$ as follows: Consider the 3-moduli set $\{P_1, P_2, P_3\} = \{2^{2n+2} - 1,\ 2^{2n+1} - 1,\ 2^n\}$ with three corresponding residues (x_1, x_2, x_3). For design the residue to binary converter for the proposed scheme, firstly need to prove that the modulus in the proposed modulus set $\{2^{2n+2} - 1,\ 2^{2n+1} - 1,\ 2^n\}$are in fact pair wise relatively prime for the validity of the RNS. Next, should to find the multiplicative inverses, and then the values of the multiplicative inverses and moduli set must substitute in conversion algorithm formulas. Then, the resulted Equations should be simplified and will be realized using hardware components such as full adders and logic gates. Based on Euclid's Theorem, we have:

$$\mathrm{gcd}\ (\mathrm{a}, \mathrm{b}) = \mathrm{gcd}\ (\mathrm{b}, \mathrm{a \bmod b}), \mathrm{a} > b \tag{7}$$

Hence,

$$\mathrm{gcd}(2^{2n+2} - 1, 2^{2n+1} - 1) = \mathrm{gcd}\ (2^{2n+1} - 1, 1) = 1 \tag{8}$$

$$\mathrm{gcd}(2^{2n+2} - 1, 2^n) = \mathrm{gcd}\ (2^n, -1) = 1 \tag{9}$$

$$\mathrm{gcd}(2^{2n+1} - 1, 2^n) = \mathrm{gcd}(2^n, -1) = 1 \tag{10}$$

Since the greatest common divisors are 1, thus the numbers $2^{2n+2} - 1,\ 2^{2n+1} - 1,\ 2^n$ are relatively prime together. In what follows using three propositions, the closed form expressions for the multiplicative inverses under the MRC are derived that form the basis of our algorithm for the reverse converter.

Proposition 1: The multiplicative inverse of $(2^{2n+2} - 1)$ modulo $(2^{2n+1} - 1)$ is $k_1 = 1$.

$$Proof{:}\ |2^{2n+2} - 1|_{2^{2n+1}-1} = 1 \tag{11}$$

Proposition 2: The multiplicative inverse of $(2^{2n+2} - 1)$ modulo (2^n) is $k_2 = -1$.

$$Proof{:}\ |-2^{2n+2} + 1|_{2^n} = 1 \tag{12}$$

Proposition 3: The multiplicative inverse of $(2^{2n+1} - 1)$ modulo (2^n) is $k_3 = -1$.

$$Proof{:}\ |-2^{2n+1} + 1|_{2^n} = 1 \tag{13}$$

Therefore, let the values $k_1 = 1,\ k_2 = -1$, $\mathrm{k_3} = -1$, $\mathrm{P_1} = 2^{2n+2} - 1$, $P_2 = 2^{2n+1} - 1$, $\mathrm{P_3} = 2^n$ in Equations 2 to 5 and we have:

$$X = x_1 + \mathrm{P_1}\,(\mathrm{V_2} + \mathrm{V_3}\, P_2) = x_1 + (2^{2n+2} - 1)(V_2 + (2^{2n+1} - 1)V_3) \tag{14}$$

$$V_1 = x_1 \tag{15}$$

$$V_2 = |(x_2 - x_1)\, |P_1^{-1}|_{P_2}|_{\mathrm{P}_2} = |(x_2 - x_1)|_{2^{2n+1}-1} \tag{16}$$

$$V_3 = |((x_3 - x_1)|P_1^{-1}|_{P_3} - V_2)\, |P_2^{-1}|_{P_3}|_{\mathrm{P}_3} = |(x_3 - x_1 + V_2)\,|_{2^{\mathrm{n}}} \tag{17}$$

Now, for designing an efficient reverse converter based on the proposed three modulus set $\{2^{2n+2}-1,\ 2^{2n+1}-1,\ 2^{n}\}$, firstly we must to design V_2 by simplify Equation 16, then by simplify Equation 17, design V_3 and finally design X based on Equation 14. For design and implementation of V_2,with simplifying Equation 16, we have:

$$V_2 = \left||(x_2 - x_1)|P_1^{-1}|_{P_2}\right|_{P_2} = |x_2 - x_1|_{2^{2n+1}-1} = |x_2|_{2^{2n+1}-1} + |-x_1|_{2^{2n+1}-1} = V_{21} + V_{22} \tag{18}$$

Where

$$V_{21} = |x_2|_{2^{2n+1}-1} = \underbrace{x_{2,2n}\ x_{2,2n-1} \dots x_{2,0}}_{(2n+1)bits} \tag{19}$$

$$V_{22} = |-x_1|_{2^{2n+1}-1} = \left\{\begin{matrix} \bar{\mathrm{x}}_{1,2n} \cdots \bar{\mathrm{x}}_{1,1}\ \bar{\mathrm{x}}_{1,0} + \\ \underbrace{\underbrace{1 \dots 1 . . 1}_{(2n)\mathrm{bits}}\ \bar{\mathrm{x}}_{1,2n+1}}_{(2n+1)\mathrm{bits}} \end{matrix}\right\} \tag{20}$$

For implementation of V_2based on Equations 19 and 20, we need to use of a $(2n+1)bits\ CSA\ with\ EAC\ and\ a\ (2n+1)bits\ CPA\ with\ EAC$,because we have three $(2n+1)$bits inputs. Fig. 1 shows the implementation of V_2.

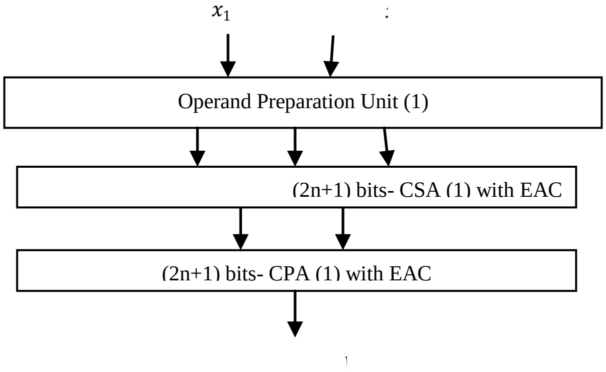
x_1
Operand Preparation Unit (1)
(2n+1) bits- CSA (1) with EAC
(2n+1) bits- CPA (1) with EAC

Fig.1 Implementation of V_2based on Equations 19 and 20

Note that for implementation of Equation 20, we need to have $(2n+2)NOT$gates that are prepared using operand preparation unit (1) $(OPU\ 1)$.

Now for design and implementation of V_3based on Equation 17, we have:

$$V_3 = \begin{pmatrix} |((x_3 - x_1)|P_1^{-1}|_{P_3}|_{P_3} = |\ (x_3 - x_1 + V_2\ )\ |_{2^n} \\ = |(x_3)|_{2^n} + |-(x_1)|_{2^n} + |V_2|_{2^n} \end{pmatrix} = V_{31} + V_{32} + V_{33} \tag{21}$$

Where,

$$V_{31} = |(x_3)|_{2^n} = \underbrace{x_{3,n-1} \dots x_{3,0}}_{(n)bits} \tag{22}$$

$$V_{32} = |-(x_1)|_{2^n} = \underbrace{\bar{\mathrm{x}}_{1,\mathrm{n}-1} \dots \bar{x}_{1,0}}_{(\mathrm{n})\mathrm{bits}} \tag{23}$$

$$V_{33} = |V_2|_{2^n} = \underbrace{V_{2,n-1} \dots V_{2,0}}_{(n)bits} \tag{24}$$

For implementation of V_3 based on Equations 22 to 24, we need to using a $(n\ bits)\ CSA\ with\ EAC$ and a $(n\ bits)\ CPA\ with\ EAC$. Fig. 2 shows the implementation of V_3 .

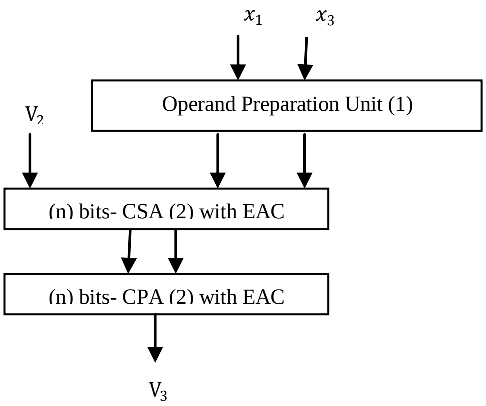
x_1
x_3
Operand Preparation Unit (1)
V2
(n) bits- CSA (2) with EAC
(n) bits- CPA (2) with EAC
V3

Fig. 2 Implementation of V_3based on Equations 22 to 24

Finally, for find X based on Equation 14, we have:

$$\begin{aligned} X &= x_1 + P_1\,(V_2 + V_3\,P_2) \\ &= x_1 \\ &\quad + (2^{2n+2} \\ &\quad - 1)\underbrace{(V_2 + (2^{2n+1} - 1)V_3\,)}_{C} \\ &= x_1 + (2^{2n+2} - 1)C \end{aligned} \qquad (25)$$

$$C = V_2 + (2^{2n+1} - 1)V_3 \qquad (26)$$

$$C = \left\{ \begin{matrix} \overbrace{\mathrm{V}_{3,n-1} \cdots \mathrm{V}_{3,0}}^{\text{n bits}}\ \overbrace{\mathrm{V}_{2,2n}}^{\text{1 bit}}\ \overbrace{\mathrm{V}_{2,2n-1} \cdots \mathrm{V}_{2,n}}^{\text{n bits}}\ \overbrace{\overline{\mathrm{V}}_{3,n-1} \ldots\ldots \overline{\mathrm{V}}_{3,0}}^{\text{n bits}} + \\ \underbrace{1 \ldots\ldots 1 \ldots\ldots 1 \ldots\ldots 1 \ldots\ldots 1 \ldots\ldots 1}_{\text{(2n+1)bits}}\ \underbrace{\mathrm{V}_{2,n-1} \cdots \mathrm{V}_{2,0}}_{\text{n bits}} \end{matrix} \right\} \qquad (27)$$

$$\begin{aligned} X &= x_1 + (2^{2n+2} - 1)C \\ &= \left\{ \begin{matrix} \overbrace{\mathrm{C}_{3n} \cdots \mathrm{C}_{n}}^{\text{(2n+2)bits}}\ \overbrace{\mathrm{C}_{n-2} \cdots \mathrm{C}_{0}}^{\text{(n-1)bits}}\ \overbrace{\overline{\mathrm{C}}_{2n+1} \cdots \overline{\mathrm{C}}_{0}}^{\text{(2n+2)bis}} + \\ \underbrace{1 \ldots 1 \ldots 1}_{\text{(2n+2)bits}}\ \underbrace{\overline{\mathrm{C}}_{3n} \cdots \overline{\mathrm{C}}_{2n+2}}_{\text{(n-1)bits}}\ \underbrace{\mathrm{x}_{1,2n+1} \cdots \mathrm{x}_{1,0}}_{\text{(2n+2)bits}} \end{matrix} \right\} \end{aligned} \qquad (28)$$

Implementation of X is shown in Fig. 3.

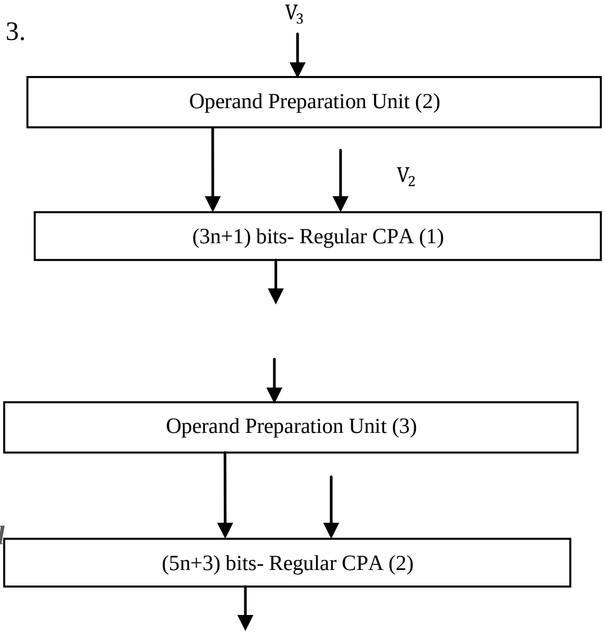
V3
Operand Preparation Unit (2)
V2
(3n+1) bits- Regular CPA (1)
Operand Preparation Unit (3)
(5n+3) bits- Regular CPA (2)

Fig. 3 Implementation of X based on Equations 27 and 28

Based on Equations 27 and 28, for implementation of X, we need to a $(3n+1) bits$ and a $(5n+3) bits$ $Regular\ CPA$. Moreover, OPU 2 and OPU 3 are needed for preparing the 1's complements in Equations 27 and 28, respectively. Addition to these, $(2n+1) bits\ and\ (2n+2) bits$ are 1 in Equations 27 and 28, respectively. Thus $(2n+2)\ and\ (2n+1)\ FAs$ can be substituted with $(2n+2)$ and $(2n+1)$ $pairs\ of\ OR\ /\ XNOR\ gates$ in Equations 27 and 28, respectively.

III. PERFORMANCE EVALUATION

In this section, hardware requirement and speed of the proposed reverse converter based on the new modulus set $\{2^{2n+2}-1,\ 2^{2n+1}-1,\ 2^n\}$ is studied. Firstly, we must to calculate the overall hardware requirement and delay of the proposed reverse converter. Then compare the results with the current reverse converters for the modulus sets with the same or less dynamic range. Area and delay requirement for implementation of each part of the proposed modulus set are shown in Table I.

TABLE I

CHARACTERIZATION OF EACH PART OF THE PROPOSED CONVERTER FOR THE NEW THREE MODULUS SET $\{2^{2N+2}-1,\ 2^{2N+1}-1,\ 2^N\}$

$Parts$	FA	NOT	$OR/XNOR$	$Delay$
OPU 1	$-$	$(2n+2)$	$-$	t_{NOT}
CSA 1	1	$-$	$(2n)$	t_{FA}
CPA 1	$(2n+1)$	$-$	$-$	$(4n+2)t_{FA}$
CSA 2	n	$-$	$-$	t_{FA}
CPA 2	n	$-$	$-$	$(2n)t_{FA}$
OPU 2	$-$	n	$-$	t_{NOT}
$R-CPA$ 1	n	$-$	$(2n+1)$	$(3n+1)t_{FA}$
OPU 3	$-$	$(2n+2)$	$-$	t_{NOT}
$R-CPA$ 2	$(3n+1)$	$-$	$(2n+2)$	$(5n+3)t_{FA}$

$$\begin{aligned} Total\ area = (8n+3)A_{FA} + \ (5n+4)A_{NOT} \\ + \ (6n+3)A_{OR} \\ + \ (6n+3)A_{XNOR} \end{aligned} \qquad (29)$$

$$Total\ delay = (14n+8)t_{FA} + \ 3t_{NOT} \qquad (30)$$

Comparison between the proposed reverse converter and current reverse converters for the modulus sets with (5n) and (4n)-bits dynamic range, in terms of area and delay is shown in Table II.

TABLE II

AREA AND DELAY COMPARISON BETWEEN THE PROPOSED REVERSE CONVERTER AND RELATED WORKS

	$Area\ (A_{FA})$	$Delay\ (t_{FA})$
[16]	$n^2+12n+12$	$16n+22$
[19]	$(5n^2\ +43n/6)+16n-1$	$18n+17$
$[20]-1$	$23n+11$	$16n+14$
$[20]-2$	$2.5n^2+\ 25.5n+12$	$18n+23$
$Proposed$	$8n+3$	$14n+8$

IV. CONCLUSIONS

The paper presents a new three modulus set $\{2^{2n+2}-1,\ 2^{2n+1}-1,\ 2^{n}\}$ with (5n)-bits dynamic range for residue number systems applications. The modules in the proposed modulus set have closed-form multiplicative inverse, thus an efficient residue to binary converter based on the proposed modulus using mixed radix conversion algorithm designs and implements. Comparison with the current reverse converters in the literatures demonstrates the proposed reverse converter has excellence in both terms of hardware saving and speed of operations.

REFERENCES

[1] T. Stouratitis and V. Paliouras, "Considering the alternatives in low-power design," *IEEE Circuits and Devices*, vol. 7, pp. 23-29, 2001.

[2] W. Wei, M.N.S. Swamy and M.O. Ahmad, "RNS application for digital image processing," *In Proc. of the 4th IEEE international workshop on system-on-chip for real time applications, Canada* ,2004, pp.77-80.

[3] S. Yen, S. Kim, S. Lim and S. Moon, "RSA speedup with Chinese remainder theorem immune against hardware fault cryptanalysis," *IEEE Transactions on Computers*, vol. 52, no. 4, pp. 461-472, 2003.

[4] E. Kinoshita and K. Lee, "A residue arithmetic extension for reliable scientific computation," *IEEE Transactions on Computers*, vol. 46, no. 2, pp. 129-138, 1997.

[5] T. Toivonen and J. Heikkila, "Video filtering with fermat number theoretic transforms using residue number system," *IEEE Transactions on Circuits, Systems and Video Technology*, vol. 16, pp. 128-135, 2006.

[6] D.M. Schinianakis, A.P. Kakarountas and T. Stoiraitis, "A new approach to elliptic curve cryptography: an RNS architecture," *IEEE Mediterranean electronical conference, Spain,* May 16-19, 2006, p.1241-5.

[7] L.L. Yang and L. Hanzo, "A residue number system based parallel communication scheme using orthogonal signaling: part I- system online," *IEEE Transactions on Vehicular Technology*, vol. 51, pp. 1534-46, 2002.

[8] R. Chaves and L. Sousa, "RDSP: A RISC DSP based on residue number system," *In: Proc. Euromicro symposium on digital systems design: architectures, methods, and tools, Antalya, Turkey*, 2003, p.128-35.

[9] A.S. Molahosseini, C. Dadkhah, K. Navi and M. Eshghi, "Efficient MRC-based residue to binary converters for the new moduli sets $\{2^{2n}, 2^{n}-1, 2^{n+1}-1\}$ and $\{2^{2n}, 2^{n}-1, 2^{n-1}-1\}$," *IEICE Transactions on Information and Systems*, vol. E92-D, no. 9, pp. 1628-1638, September 2009.

[10] K.M. Elleithy and M.A. Bayoumi, "Fast and flexible architectures for RNS arithmetic decoding," *IEEE Transactions on Circuits and Systems-II*, vol. 39, no. 4, pp. 226-235, 1992.

[11] C.H. Huang, "A fully parallel mixed radix conversion algorithm for residue number applications", *IEEE Transactions on Computer*, vol. 32, no. 4, pp. 398-402, 1983.

[12] P.V.A. Mohan, "Evaluation of fast conversion technique for binary-residue number systems", *IEEE Transactions on Circuit and Systems-I*, vol. 45, no. 10, pp. 1107-1109, 1998.

[13] P.V.A. Mohan, "The digit parallel method for fast RNS to weighted number system conversion for specific moduli $(2^{n}-1, 2^{n}, 2^{n}+1)$," *IEEE Transactions on Circuits and Systems-II*, vol. 47, no. 9, pp. 972-974, 2000.

[14] P.V.A. Mohan, "Breaking the 2n-bit carry propagation barrier in residue to binary conversion for the $(2^{n}-1, 2^{n}, 2^{n}+1)$ moduli set," *IEEE Transactions on Circuits and Systems-II,* vol. 48, no. 8, pp. 1031-1035, 2001.

[15] M. Bhardwaj, T. Srikanthan and C.T. Clarke, "A reverse converter for the 4-moduli superset $\{2^{n}-1, 2^{n}, 2^{n}+1, 2^{n+1}+1\}$," *Proc. IEEE Symposium on Computer Arithmetic*, 1999.

[16] P.V.A. Mohan and A.B. Premkumar, "RNS-to-binary converters for two four-moduli set $\{2^{n}-1, 2^{n}, 2^{n}+1, 2^{n+1}-1\}$ and $\{2^{n}-1, 2^{n}, 2^{n}+1, 2^{n+1}+1\}$," *IEEE Transactions on Circuits and Systems,* vol. 54, no. 6, pp. 1245-1254, 2007.

[17] A. Hariri, K. Navi and R. Rastegar, "A new high dynamic range moduli set with efficient reverse converter, " *Elsevier Journal of Computers and Mathematics with Applications*, vol. 55, no. 4, pp. 660-668, 2008.

[18] F.J. Taylor, "Residue arithmetic: A tutorial with examples," *IEEE Computer Magazine*, vol. 17, no. 5, pp. 50-62, 1986.

[19] B. Cao, C.H. Chang and T.H. Srikanthan, "A residue to binary converter for a new five moduli set," *IEEE Transactions on circuits and systems – I: regular papers*, vol. 54, no. 5, pp. 1041-1049, 2007.

[20] P.V.A. Mohan, "New reverse converters for the moduli set $\{2^{n}-3, 2^{n}-1, 2^{n}+1, 2^{n}+3\}$," *Elsevier/ International Journal of Electronics and Communications (AEU),* vol. 62, no. 9, pp. 643-658, 2008.