International Journal of Advanced Information Science and Technology (IJAIST) ISSN: 2319:268
Vol.3, No.3, March 2014 DOI:10.15693/ijaist/2014.v3i3.9-14

Energy Efficient Processor Using The Advanced Residue Number System And Chinese Remainder Theorem

SANDHYA.C[1] DHARANI KUMAR M[2]
PG SCHOLAR ASSISTANT PROFESSOR
DEPARTMENT OF ECE
KARPAGAM UNIVERSITY

Abstract—This work presents some results on multiple errordetection and correction based on the Redundant Residue NumberSystem (RRNS). RRNS is often used in parallel processingenvironments because of its ability to increase the robustnessof information passing between the processors. The proposedmultiple error correction scheme utilizes the Chinese RemainderTheorem (CRT) together with a novel algorithm that significantlysimplifies the error correcting process for integers. An extensionof the scheme further reduces the computational complexitywithout compromising its error correcting capability. Proofs andexamples are provided for the coding technique which be implemented using Cadence virtuoso tool of 180nm CMOS process.

Index Terms—Arithmetic codes, error correction coding, maximumlikelihood decoding, redundant number systems, residuecodes.

INTRODUCTION

The integrity of information passing through moderndigital systems such as filters and arithmetic units isof utmost importance different coding schemes have beenemployed to achieve reliable and efficient transmission ofdata through these systems [1] an area of particular interestis error detection and correction using a Redundant ResidueNumber System. A Residue Number System (RNS)for integers describes methods of representing an integer as aset of its remainders or residues. Error control is achieved byaddition of extra residue hence the term RRNS and the RRNS code used in this work uses the Chinese RemainderTheorem (CRT) as a means of recovering the integerfrom a set of its residues.

Error correcting codes based onthe CRT are attractive because of their ability to performcarry-free arithmetic and lack of ordered significance amongthe residues [2]. Significant work concerning RRNS has beencarried out by numerous parties after the initial push by [3],[4]. They introduced some of the concepts relatedto this error correction technique such as the terms legitimaterange and illegitimate range for consistency checking.

In [1],a discussion of a single residue error correction algorithmis given. [6] and [7] addressed the problem of double andmultiple residue error correction, respectively.There are generally two different strategies employed tocorrect errors in a redundant residue code. The first method calculates the syndromes of received residues and then comparesthem with a set of predetermined observations. Fromthere, conclusions are drawn and the appropriate integerrecovery algorithm is performed. This is similar to algorithmsgiven in [1] and [7].

The second method begins by recoveringthe erroneous integer from the received residues using theCRT. Subsequently, an error value is estimated using eithercontinued fractions or integer programming. The correct integeris thus recovered by subtracting the error value from theerroneous integer. [5] And [6] suggested algorithms using this strategy.In this paper, a novel error correction scheme based onthe second strategy is proposed. This scheme is similarto that in [5] and [6].

However, the proposed scheme issignificantly simpler and does not require any complicatedoptimization algorithms. Briefly, in this scheme, the erroneousinteger that is computed from its residues is used in a simplemodular calculation that is iterated until the original integeris recovered. The algorithm is straightforward and easier toimplement. Furthermore, the theory and concept of this errorcorrection scheme is extended to make it more efficient andless computationally intensive.The presentation of this work can be divided into five sections.In Section II, some initial concepts and materials relatedto the RRNS and CRT are given. The major contributionof this paper, which is the multiple error correction scheme,is given in Section III.

In this section, mathematical proofsand examples are given to illustrate the salient features ofthe error correction scheme. Section IV discusses techniquesthat are used to improve performance of the scheme, withoutcompromising its error correcting capabilities. Conclusionsand recommendations are given in Section V.

REDUNDANT RESIDUE NUMBER SYSTEMS AND CHINESE REMAINDER THEOREM

To enable error correcting capabilities in RRNS, somerelevant background and terminologies must be first defined.To begin, a set of n pairwise relatively prime positive integersm1,m2, . . . , mi,mi+1, . . .,mn called moduli is selected.

Note that the term moduli is the plural of modulus. Themoduli mi are chosen such that, the greatest common divisor,gcd(mi,mj) = 1 for each pair of i and j with i = j andm1 < m2 < . . . < mi < mi+1 < . . . <mn. Fromthis set of n moduli, the first k moduli form a set of nonredundantmoduli while the last r = n − k moduli form aset of redundant moduli [1]. These sets of moduli are used todefine the following,Mk = m1MR =N i=k+1miM =ni=1mi = MK ·MR (2)for i = 1, 2, k, k + 1, . . . , n. It can be seen that MK isthe smallest product of k different mi's.

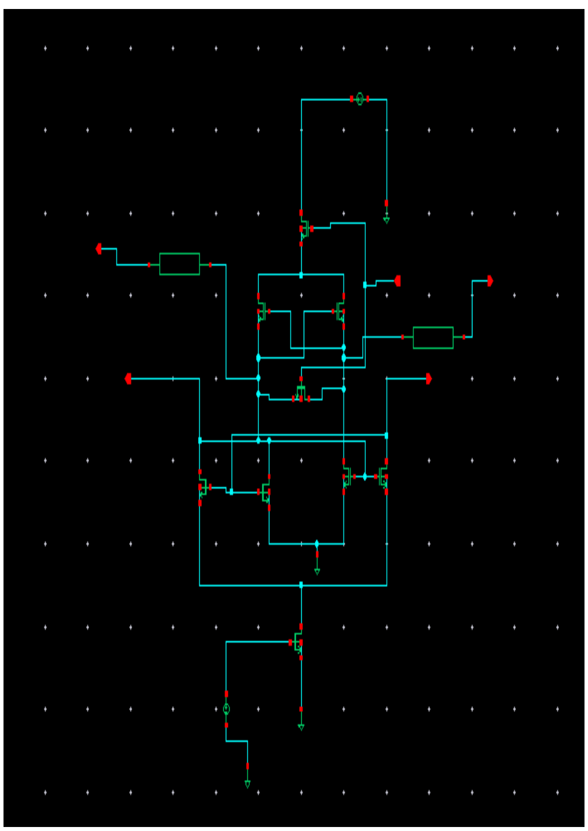

Fig.1. Scheme for the Number system generation

As with other error correction codes, the redundant components are used for error detection and correction. Without loss of generality, an integer X in the range of [0,M) where M is as defined in (2), can be uniquely represented by a residue vector x = {x1, x2, . . . , xn} using X ≡ xi (modmi) (3) for i = 1, 2, . . . , k, k+1, . . . , n. With (3), each of the residues xi corresponds to X modulo mi such that 0 ≤ xi < mi. As shown in the fig.1.

However, for error correction to work, X has to be selectedfrom the range of [0,MK) instead, where MK is from (1). Indoing so, the residue vector x can be divided into two parts,namely the first k residues called information residues and theremaining r residues called redundant residues [1].Without loss of generality again, when a residue vectorx is given, the corresponding integer X can be uniquelydetermined by simultaneously solving all n linear congruencesin (3). The problem of simultaneously solving a set of linearcongruences is simplified by using the CRT as shown belowX =ni=1xiMiaimodM (4)whereMi = Mmiand ai = M−1i modmifori = 1, 2, . . ., n. The integersai are also known as themultiplicative inverses of Mimod mi. If X is selected fromthe range of [0,MK), any k residues out of the total n residuesfrom the residue vector x, where n > k should be sufficientin recovering the original integer X.From [1], when the integer X is chosen from the rangeof [0,MK), the resulting redundant residue code can beconsidered semiinear.Theorem 1: A code Ω based on a redundant residue numbersystem has the minimum nonzero Hamming weight wtmin ≥r + 1 and minimum distance dmin ≥ r + 1 [8].

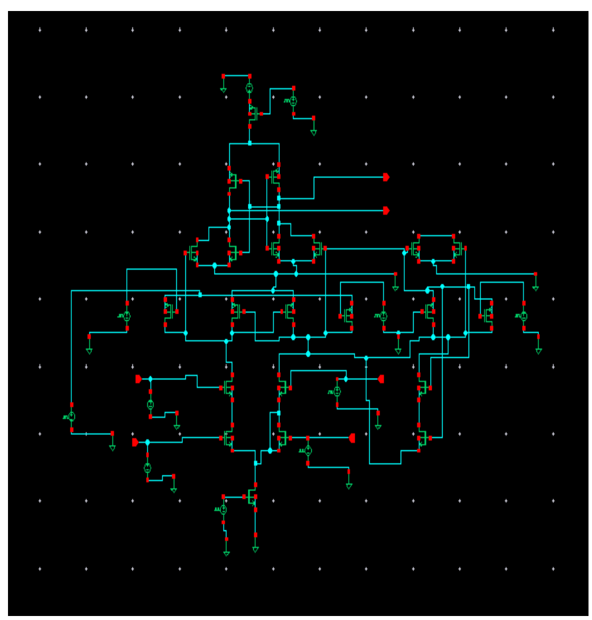

Fig.2. NUMBER SYSTEM MODULE

According to Theorem 1, since the minimum distance can have the value of r + 1, the code Ω can be considered maximum distance separable (MDS). MDS codes are codes that have dmin = r + 1. Theorem 2: A code Ω based on a redundant residue number system can correct up to t errors; t ≤ r/2 where is the largest integer less than or equal to ∗ [8]. MDS codes are attractive because they are optimal whereby they can correct the maximum amount of errors t, with the least number of redundancies. Code generation circuit as shown in fig.2.

MULTIPLE ERROR CORRECTION SCHEME

For the multiple error correction scheme, first consider aredundant residue code with a set of moduli mi. An integerX is selected from the range [0,MK) and the residue vector isx = {x1, x2, . . . , xn}. n and k are chosen such that Theorem2 holds, thus allowing this code to correct up to t errors.From here onwards, let the range [0,MK) be termed as thelegitimate range while its counterpart, the range [MK,M) betermed as the illegitimate range. Suppose that t errors havebeen introduced into the vector y when it passes through apotentially noisy system. The resulting vector is y, that isy = x +e{y1, . . . ,yn} = {x1, . . . , xn}+ {eu1, . . . , 0, eu2, . . . , eut} (5)where 0 ≤ euj<muj for 1 ≤ j ≤ t. The errorvalues are eu1, eu2, . . . , euj, euj+1, . . .eut and the subscriptsu1, u2, . . . , uj, uj+1, . . . , ut are the positions of errors withiny. Upon receiving the vector y, error detection is first performedby determining whether y is a valid vector.

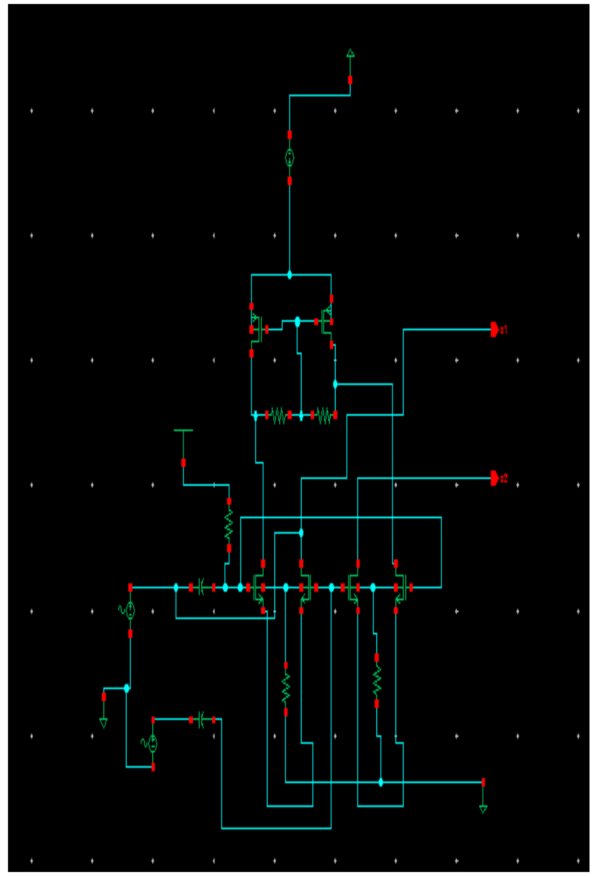

Fig.3. Number system schedule module

This canbe accomplished by computing the corresponding integer Yusing a formula based on (4), which isY =ni=1yiMiaimodM (6)where Mi and ai are as defined earlier for (4). If the recoveredY is within the legitimate range, then y is a valid vector andno further steps need to be carried out. On the other hand, if Yis in the illegitimate range, it can then be concluded that y haserrors in its residue. When there are errors, the relationshipbetween X and Y isX ≡ (Y − E) (modM) , 0 ≤ E ≤ M. (7)In (7), E is the amount of error that has propagated into theX resulting in the erroneous Y . The magnitude of the errorE can be calculated using the CRT and is determined to beE ≡tj=1eujMujauj (modM) (8)where Muj,muj and auj are the corresponding values of Mi,mi and ai for i = uj.To simplify the decoding problem, let E in (8) be expressedin its expanded form, givingE ≡eu1Mmu1au1 + . . . + eutMmutaut(modM) . (9)Let M from (2) be expressed asM =ni=1mi =utα=u1mα ·ln−tβ=l1mβ (10)where u1, u2, . . . , uj, uj+1,. . . , ut are the positions of residueswith errors and l1, l2, . . . , ln−t are the remaining positionswithout errors inside the vector y. By substituting (10) into(9), (11) is obtained. Continue by lettingg = eu1ut=u1α=u1mα · au1 + . . . + eut·utα=u1α=utmα · autZc =ln−tβ=l1mβ

EXTENSION TO ERROR CORRECTION SCHEMES BASEDON THE RRNS

While error correction algorithm has been proven to work,the recovery process can still be computationally intensive. Alarge number of iterations is sometimes required to correctlyguess the positions of the errors. The systematic approachof trying all possible combinations means that it will take atmost p = nCt trials.

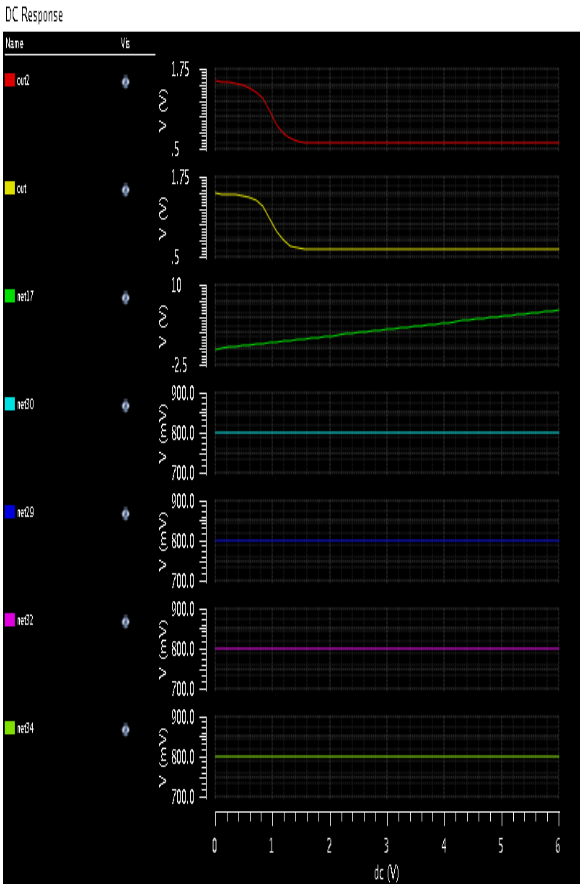

Fig.4. Transient analysis

The variables n and t are the number of residues and correctable errors for a (n, k) code, respectively. Designing a code that can correct more errors requires that the number of residues be increased too. As a result, the number of trials p will grow, increasing the computational overhead. To remedy this shortcoming, the multiple error correction algorithm presented earlier in Section III needs to be modified. Firstly, recall that exactly t errors can be corrected using (13). In addition, it has been shown that any errors less than t can also be corrected with (13).

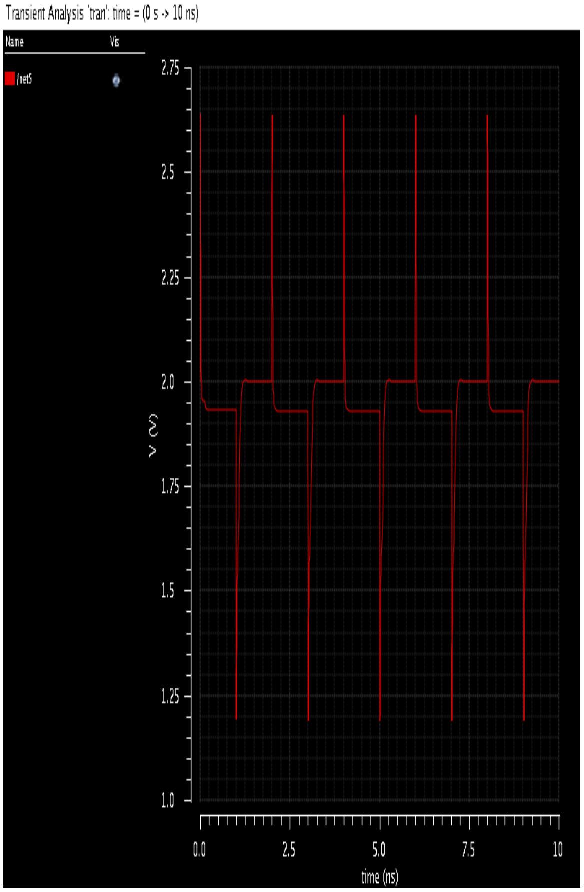

Fig.5. Transient analysis

This is possible as long as Zc isthe product of any (n − t) moduli corresponding to residueswithout errors.If the multiple error correction algorithm was set to correcto errors where o > t,any errors less than o can also becorrected. However, ambiguity will arise because more thanone possible solution will fall within the legitimate range. Theproblem is caused by the fact that the algorithm is attemptingto correct more errors then it possibly can.

International Journal of Advanced Information Science and Technology (IJAIST) ISSN: 2319:268
Vol.3, No.3, March 2014 DOI:10.15693/ijaist/2014.v3i3.9-14

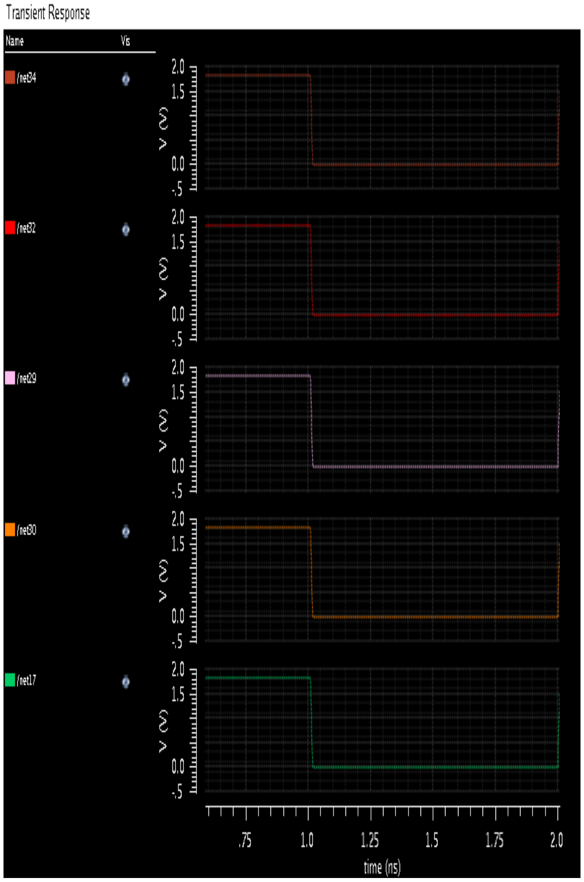

Fig.6. Module transient analysis

Therefore, thesolutions are for residues with γ, t+1, t+2, o errors whereγ ∈ {0, 1, . . . , t−1, t}. To resolve the ambiguity, solutions forresidues with t+1, t+2, o errors will have to eliminated.A very simple way of eliminating nonsensical solutions isto use the maximum likelihood decoding (MLD). Let the setof solutions of a scheme that has been set to correct o errors The only value of Vi that has a Hamming distance whichis less than or equal to t = 2 is 51. Therefore, the modifiederror correction algorithm has correctly recovered the originalinteger.

Table I

K0	**2.5V**	**2.25V**	**0.8V**	**1.5V**
Length	14	12	8	6
Soft error 1	0%	0.9%	6.5%	13%
Soft error 2	0%	0.8%	5.5%	11%
Soft error 3	0%	0.7%	5.5%	10%
Soft error 4	0%	0.6%	4.5%	9%

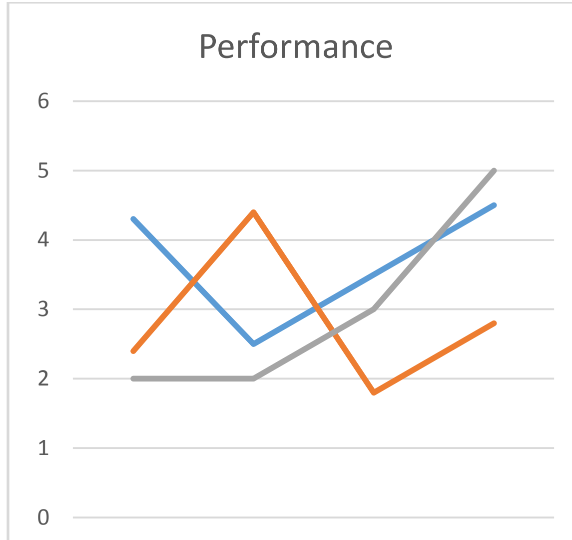

Fig.6. Comparison analysis

Although the total number of iterations shown inthis example is three, the original integer could have beenrecovered in the second iteration.The overall performance gain of the modified algorithmcompared to the original algorithm is shown in Fig. 1. Theeffects of the modified algorithm are more significant whenthe total number of correctable errors, t is larger. Note thatthe number of trials for the modified algorithm f, is obtainedexperimentally and are obtained for worst case situationswhere the maximum number of iterations need to carried out.

CONCLUSIONS

The single error correction scheme is significantly simplerand does not require any complicated optimization algorithmsuch as those used by [6]. Furthermore, the algorithm is quitestraightforward and easy to implement as it has been shown inthe procedural codes. Unlike the scheme proposed by [1], thisalgorithm can be easily improved upon to correct multipleerrors without major changes in the algorithm. However,the proposed multiple error correction scheme does requiremore iterations in order to correct the errors. This limitation increases the computational overhead in terms of resourcesand time. In addition, when using the CRT, large numbersmay be encountered that can further reduce the performanceof the algorithm. It be implemented using a Cadence virtuoso 180nm technology.

REFERENCES

[1] Jienan Chen and Jianhao Hu," Energy-Efficient Digital Signal Processing via Voltage-Overscaling-Based Residue Number System" , IEEE Transactions On Very Large Scale Integration (Vlsi) Systems, Vol. 21, No. 7, July 2013,PP 1322-1332.

[2] L. L. Yang and L. Hanzo, "Redundant residue number system basederror correction codes," in Proc. 54th Veh. Technol. Conf., 2001, pp.1472-1476.

[3] F. Barsi and P. Maestrini, "Error correcting properties of redundantresidue number systems," IEEE Trans. Comput., vol. 81, pp. 307-315,Mar. 1973.

[4] D. M. Mandelbaum, "Error correction in residue arithmetic," IEEETrans. Comput., vol. 21, pp. 538-545, June 1972.

[5] D. M. Mandelbaum, "On a class of arithmetic codes and a decodingalgorithm," IEEE Trans. Inform. Theory, vol. 22, pp. 85-88, Jan. 1976.

[6] O. Goldreich, D. Ron, and M. Sudan, "Chinese remaindering witherrors," IEEE Trans. Inform. Theory, vol. 46, pp. 1330-1338, July 2000.

[7] J. D. Sun and H. Krishna, "A coding theory approach to error control inredundant residue number systems. Part II: Multiple error detection andcorrection," IEEE Trans. Circuits Syst., vol. 39, pp. 18-34, Jan. 1992.

[8] C. Ding, D. Pei, and A. Salomma, Chinese Remainder Theorem:Applications in Computing, Coding, Cryptography. Singapore: WorldScientific Publishing, 1996.

[9] P. E. Beckmann and B. R. Musicus, "Fast fault-tolerant digital convolutionusing a polynomial residue number system," IEEE Trans. SignalProcessing, vol. 41, pp. 2300-2313, July 1993.

[10] A. J. Menezes, P. C. van Oorschot, and S. A. Vanstone, Handbook ofApplied Cryptography. Boca Raton, FL: CRC Press, 1996.

[11] R. A. Abdallah and N. R. Shanbhag, "Error-resilient low-power viterbidecoder architectures," IEEE Trans. Signal Process., vol. 57, no. 12, pp.4906–4917, Dec. 2009.

[12] M. Nekili, Y. Savaria, and G. Bois, "Spatial characterization of processvariations via MOS transistor time constants in VLSI and WSI," IEEEJ. Solid-State Circuits, vol. 34, no. 1, pp. 80–84, Jan. 1999.

[13] S. Ashish, S. Dennis, and B. David, Statistical Analysis and Optimizationfor VLSI: Timing and Power. Berlin, Germany: Springer-Verlag, 2005.

[14] G. L. Bernocchi, G. C. Cardarilli, A. Del Re, A. Nannarelli, and M. Re,"Low-power adaptive filter based on RNS components," in Proc. IEEEInt. Symp. Circuits Syst., May 2007, pp. 3211–3214.

[15] I. Kouretas and V. Paliouras, "RNS multi-voltage low-power multiplyaddunit," in Proc. 17th IEEE Int. Conf. Electron., Circuits, Syst., Dec.2010, pp. 9–12.

[16] V. T. Goh and M. U. Siddiqi, "Multiple error detection and correctionbased on redundant residue number systems," IEEE Trans. Commun.,vol. 56, no. 3, pp. 325–330, Mar. 2008.

Author Profile

Sandhya .C pursuing Master of Engineering VLSI Desigin in Karpagam University, Coimbatore. Completed Bachelor of Engineering Electronics and Instrumentation Engineering from Sri Ramakrishna College of Engineering, Coimbatore. Bharat Power conversion, Coimbatore for past two years. Her research fields includes low power, VLSI.

M.Daranikumarworking as a Assistant Professor in Karpagam University, Coimbatore, India. Completed M.E.at electronics and communication engineering in Anna University of technology, Coimbatore, India. His research interest includes Communication Systems, Testing of VLSI, Digital Electronics, CMOS VLSI Design.