IMPLEMENTATION OF EFFICIENT MODULAR ADDERS BASED ON ADAPTIVE RESIDUAL NUMBER SYSTEM (ARNS)

M.Sudha Madhuri, E.C.E (Vlsi & Es), M.tech, Vsm college of Engineering Ramachandrapuram, madhuri.masina@gmail.com
V.Ravindra , Associate professor , Vsm college of engineering Ramachandrapuram, Ravindravundavalli@gmail.com

ABSTRACT

The logic gates electronic circuits computing the arithmetic operations for various multimedia applications. Therefore, reversible logic gates are necessary for advanced ultra-low power requests. The recent VLSI technology mainly depending on adders and multiplayers functionality. Reversible logic circuits are major examples of quantum computing. The adaptive residual number system (ARNS) is an efficient tool to offering the fault tolerance and parallel addition and multiplication operations. In this research work novel ARNS and reversible logic circuits are utilized to improves the performance of VLSI chip design. The modulo 2^n– 1 summer circuits with the help of reversible logic and ARNS blocks are used for multiplayer operations. At final comparing the existed methods through adaptive RNS model. Therefore simulation results outperform the performance measures and gives the accurate outcomes.

1. Introduction

Reversible logic is a computing paradigm that has attracted significant attention in recent years due to its properties that lead to ultra-low power and reliable circuits. Reversible circuits are fundamental, for example, for quantum computing. Since addition is a fundamental operation, designing efficient adders is a cornerstone in the research of reversible circuits. Residue Number Systems (RNS) has been as a powerful tool to provide parallel and fault-tolerant implementations of computations where additions and multiplications are dominant. In this paper, for the first time in the literature, we propose the combination of RNS and reversible logic. The parallelism of RNS is leveraged to increase the performance of reversible computational circuits. Being the most fundamental part in any RNS, in this work we propose the implementation of modular adders, namely modulo 2n-1 adders, using reversible logic. Analysis and comparison with traditional logic show that modulo adders can be designed using reversible gates with minimum overhead in comparison to regular reversible adders.

Researchers in academia and industry believe that Moore's law is ending, and even newly delivered deep-submicron transistors are not significantly more efficient than their previous generations [1]. Therefore, new computing paradigms should be investigated in order to overcome the

predicted performance wall which will be reached in 2020 [1]. This rebooting of computing has to be based on novel methods at different computing levels of design abstraction, including arithmetic and circuit level, in order to address the challenges of the emerging applications such as deep convolutional neural network (DNN) and internet-of-things (IoT) [2].

2. Literature survey

Residue Number System (RNS) is one unconventional number system [3] that can provide fast and low-power implementation of additions and multiplications. RNS is a different approach of dealing and representing numbers that provide parallelism at arithmetic level [4]. This number system has been applied to achieve parallel and efficient implementations for asymmetric cryptographic and digital signal processing (DSP) [5]. RNS is used nowadays to achieve also energy-efficient and high-performance implementation of various emerging applications, such as deep neural networks, communication networks and cloud storage [3]. However, current implementations of RNS systems, on ASICs and FPGAs, are based on the CMOS technology, which is reaching its limit. Alternative methods and technologies, such as nanoelectronic, are considered to be used.

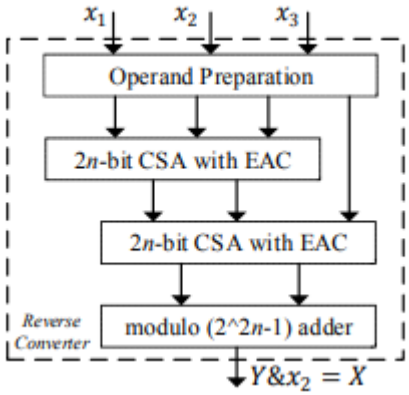


Fig. 1. The full reverse converter for the moduli set {2n -1, 2n+k , 2n +1}

One of these alternatives is Reversible Computing (RC) [6], which can provide ultra-low power computational circuits. In this paper, we propose the joint usage of these two unconventional computing approaches, Residue Number System and Reversible Computing, to achieve ultra-efficient computing paradigm for the emerging applications. The ability of RNS to perform highly parallel and carry-free arithmetic is well suited for taking advantage of the features of reversible circuits. In other words, reversible logic can be efficiently used to implement RNS circuits. However, since all the available RNS structures are designed for ASIC implementation, rethinking of RNS architectures should be performed to adapt them to the properties of reversible circuits. The fundamental part of RNS systems is modular addition, since all parts of RNS including forward and reverse conversion are based on modular additions. Hence, the first step to implement RNS systems

based on reversible circuits requires the design of efficient modular adders using reversible logic gates. This paper presents the first implementation of modulo 2n -1 adders based on reversible gates. For these modular adders, which are frequently used in RNS structures, parallel-prefix and ripple-carry architectures are considered.

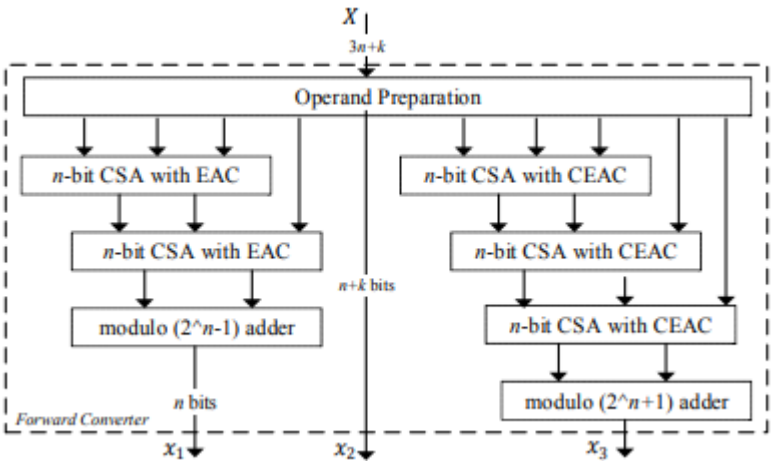


Figure: 2 forward converter for the moduli set{2n -1, 2n+k , 2n +1}

Most of the mentioned RNS operations are implemented using 3-to-2 carry-save adders (CSAs) with end-around carries (EACs) and 2-to-1 modular adders [14]. A full hardware design of RNS with moduli set {2n -1, 2n+k , 2n +1} is reported in [7], and herein forward and reverse converters for this moduli set are depicted in Figs. 1 and 2, respectively. It can be observed that CSAs and carry-propagate modulo 2n -1 adders are the components required to implement a full RNS architecture, since arithmetic in a channel also requires modulo adders and multipliers. Thus, to have an efficient modular adder is fundamental for RNS-based applications.

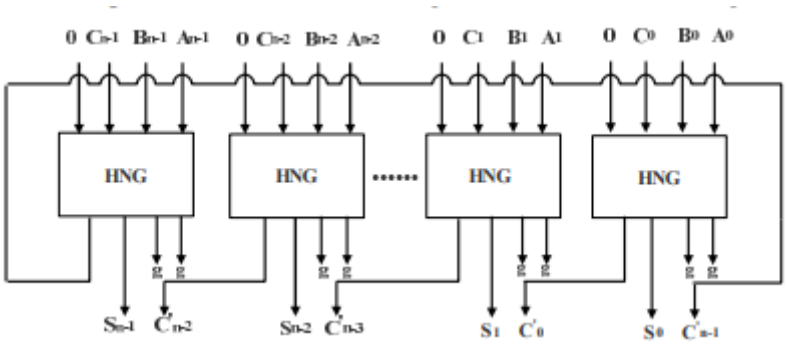


Fig. 3. The CSA with EAC using HNG reversible gates.

The quantum depth and cost of a HNG gate is 5Δ and 6, respectively [22]. Therefore, the total quantum depth and cost of a n-bit CSA with EAC will be 5Δ and 6n, respectively, since the delay of a

CSA is equal to the delay of just one FA. Besides, the final reversible circuits will have n constant inputs and 2n garbage outputs.

Since the designing of metallic interconnects is done toward the finish of the chip creation, the pivot time can be still short, a couple of days to half a month. Figure 5.9 shows an edge of an entryway exhibit chip which contains holding cushions to its left side and base edges, diodes for I/O assurance, nMOS semiconductors and pMOS semiconductors for chip yield driver circuits in the neighboring territories of holding cushions, varieties of nMOS semiconductors and pMOS semiconductors, underpass wire portions, and force and ground transports alongside contact windows.

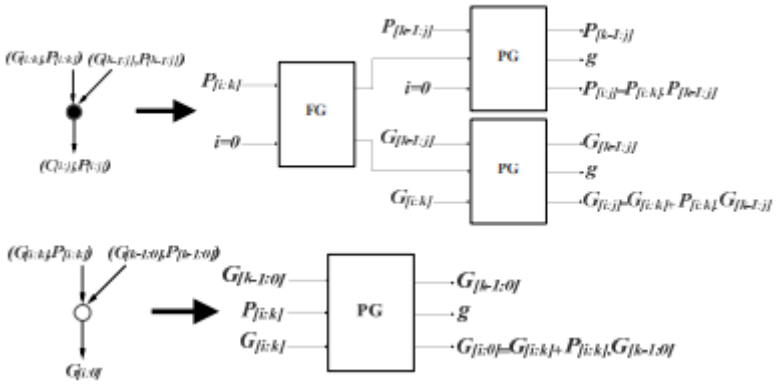


Fig: 4. internal prefix cells implementation using Peres gates

Ex1: A hello world program looks like this:

```
Module main;
    Initial
        Begin
            $display("Hello world!");
            $finish;
        end
endmodule
```

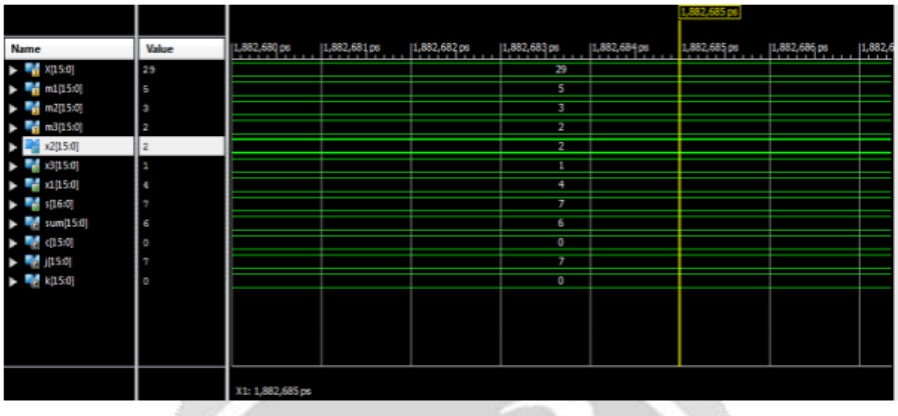
Ex2: A simple example of two flip-flops follows:

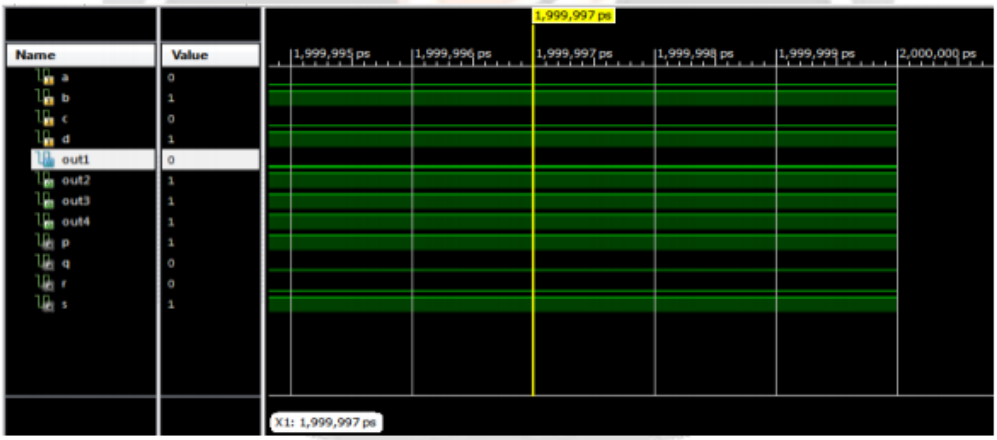
```
module toplevel(clock,reset);
    input clock;
    input reset;

     reg flop1;
     reg flop2;

   always @ (posedge reset or posedge clock)
    if (reset)
        begin
         flop1 <= 0;
        flop2 <= 1;
        end
    else
        begin
        flop1 <= flop2;
         flop2 <= flop1;
        end
endmodule
```

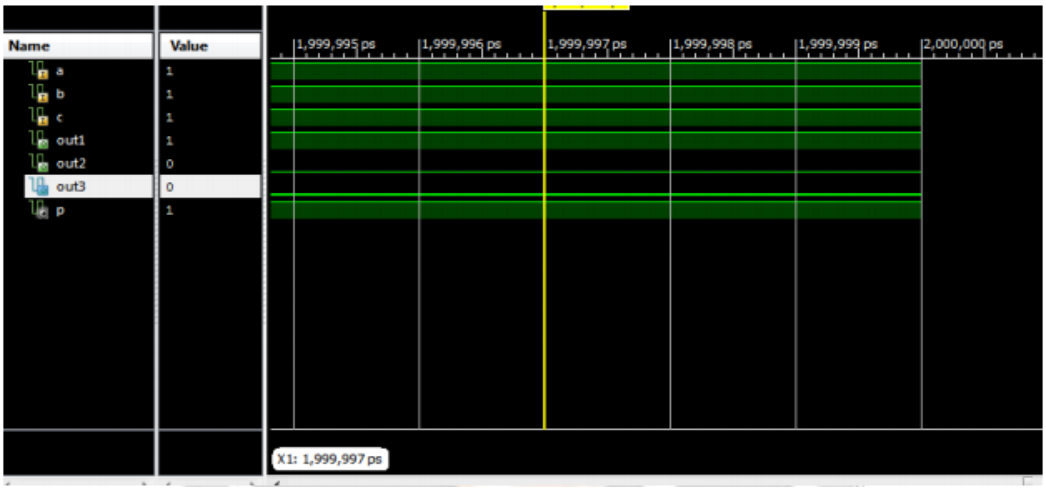
The total quantum cost and depth as well as number of constant inputs and garbage outputs of the different adders are presented in Table I. It can be seen that, as it was expected, the proposed 2n -1 modulo adders have higher cost and depth than the equivalent binary adders. The proposed prefix-based modular adders have 19.81% and 7.55% overhead in terms of cost and depth, respectively, in comparison to the regular BrentKung prefix adder for n=32. However, for the same width, RCA with EAC results in 40% and 49.2% overhead in cost and depth, respectively, in comparison to the regular RCA. Therefore, it can be concluded that designing prefix-based modular adder results in less overhead than RCA-based design, in reversible logic. Besides, it can be seen from Table I that a 3-to-2 compression unit, like CSA, which is quite frequently used in RNS circuits, can be implemented quite efficiently using reversible gates.

OUTPUT RESULTS

Type	Adders	Circuit Parameters															
		Quantum Cost				Quantum Depth (Δ)				Constant Inputs				Garbage Outputs			
		8	16	32	64	8	16	32	64	8	16	32	64	8	16	32	64
Regular [21]	Kogge-Stone	158	446	1166	2894	19	24	29	34	28	84	228	580	43	115	291	707
	Brent-Kung	104	239	518	1085	29	39	49	59	16	38	84	178	31	69	147	305
	Sklansky	196	496	1200	2816	20	25	30	35	32	80	192	448	52	128	304	704
	RCA	48	96	192	384	27	51	99	195	8	16	32	64	16	32	64	128
Modular Proposed	Brent-Kung w. EAC	136	303	646	1341	33	43	53	63	16	38	84	178	47	101	211	433
	CSA with EAC	48	96	192	384	5	5	5	5	8	16	32	64	16	32	64	128
	RCA with EAC	80	160	320	640	51	99	195	387	16	32	64	128	25	49	97	193

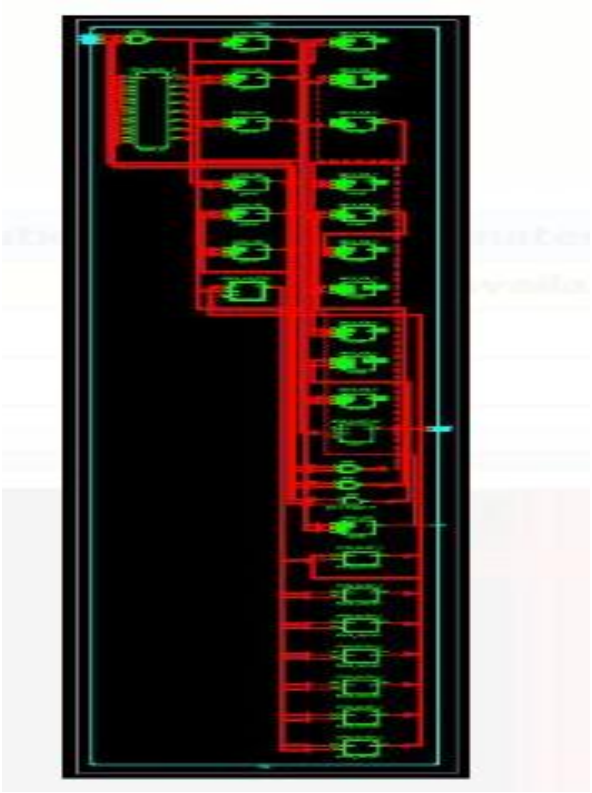




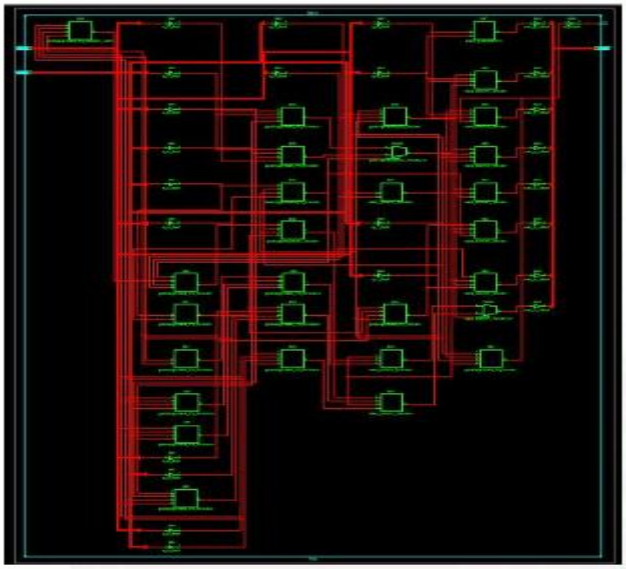


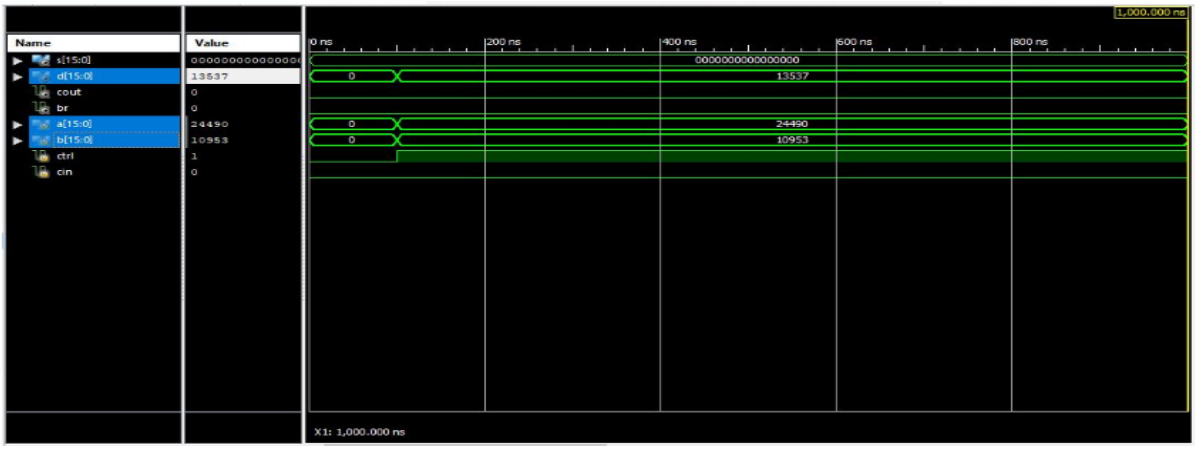
DESCRIPTION	AREA ANALYSIS	TIMING REPORT	POWER ANALYSIS
UNIVERSAL GATES-MODULO ADDER	59 LUT's	12.596ns	328.27mW
REVERSIBLE GATES-MODULO ADDER	245 LUT's	12.47ns	144.06mw

Device Utilization Summary (estimated values)			[-]
Logic Utilization	Used	Available	Utilization
Number of Slices	15	4656	0%
Number of 4 input LUTs	27	9312	0%
Number of bonded IOBs	25	232	10%



```
Data Path: a<2> to sum<2>
                                   Gate     Net
  Cell:in->out      fanout   Delay   Delay  Logical Name (Net Name)
  ----------------------------------------  ------------
   IBUF:I->O             6   1.106   0.638  a_2_IBUF (a_2_IBUF)
   LUT4:I1->O            4   0.612   0.499  bcell2/pgl2/Mxor_P3_Result1 (w4<1>)
   MUXF5:S->O            8   0.641   0.795  gcell7/pgl/Mxor_P3_Result1_f5 (N11)
   LUT4:I0->O            2   0.612   0.532  gcell7/pgl/Mxor_P3_Result2 (co_OBUF)
   LUT4:I0->O            1   0.612   0.357  Mxor_sum<2>_Result2 (sum_2_OBUF)
   OBUF:I->O                 3.169          sum_2_OBUF (sum<2>)
  ----------------------------------------
  Total                     9.573ns (6.752ns logic, 2.821ns route)
                                    (70.5% logic, 29.5% route)
```





Conclusion

This work presents the reversible design of modular adders, a basic and fundamental element of RNS-based architectures. It is shown that a modulo 2n -1 parallel-prefix adder can be designed using small overheads over regular prefix adders. The next steps, which should be considered for future work, are reformulating the adaptive residual number system (ARNS) operations, such as reverse conversion, sign detection and scaling, to adapt them to be implemented with reversible gates. They can benefit from the efficient proposed reversible-based modular adders. It is expected that this paper opens a new and substantial field of research to join modular arithmetic and reversible computing, resulting in efficient computational architectures for the post-Moore era.

REFERENCES

1. T.M. Conte, E.P. DeBenedictis, P.A. Gargini, and E. Track, “Rebooting Computing: The Road Ahead,” Computer, vol. 50, no. 1, pp. 20-29, 2017.
2. M. Alioto (Ed.), Enabling the Internet of Things: From Integrated Circuits to Integrated Systems, Springer , 2017.

3. A.S.Molahosseini, L.Sousa and C.H. Chang (Eds.), Embedded Systems Design with Special Arithmetic and Number Systems,Springer, 2017.
4. C.H. Chang, A.S.Molahosseini, A.A.Emrani Zarandi, and T.F.Tay, “Residue Number Systems: A New Paradigm to Datapath Optimization for Low-Power and High-Performance Digital Signal Processing Applications,” IEEE Circuits and Systems Magazine, vol. 15, no. 4, pp. 26-44, 2015.
5. L. Sousa, S. Antão, and P. Martins, “Combining Residue Arithmetic to Design Efficient Cryptographic Circuits and Systems,” IEEE Circuits and Systems Magazine, vol. 16, no. 4, pp. 6-32, 2016.
6. E.P. DeBenedictis, J.K. Mee, and M.P. Frank, “The Opportunities and Controversies of Reversible Computing,” Computer, vol. 50, no. 6, pp. 76-80, 2017.
7. R. Chaves and L. Sousa, “Improving RNS multiplication with more balanced moduli sets and enhanced modular arithmetic structures,”IET Computers & Digital Techniques, vol. 1, n. 5, pp. 472-480, 2007.
8. A. Hiasat, “An Efficient Reverse Converter for the Three-Moduli Set (2n+1-1, 2n , 2n -1),” IEEE Transactions on Circuits and Systems-II, vol. 64, no. 8, 2017.
9. A.S. Molahosseini, K. Navi, C. Dadkhah, O. Kavehei, S. Timarchi, "Efficient reverse converter designs for the new 4-moduli sets {2n –1, 2n , 2n +1, 22n+1–1} and {2n –1, 2n +1, 22n , 22n +1} based on new CRTs," IEEE Transactions on Circuits and Systems-I, vol. 57, no. 4, pp. 823-835, 2010.
10. P. Patronik and S.J. Piestrak, "Design of Reverse Converters for General RNS Moduli Sets {2k , 2n -1, 2n +1, 2n+1-1} and {2k , 2n -1, 2n +1, 2n-1-1} (n even)," IEEE Transactions on Circuits and Systems-I, vol. 61, no. 6, pp. 1687-1700, 2014.
11. B. Cao, C. H. Chang and T. Srikanthan, "A Residue-to-Binary Converter for a New Five-Moduli Set," IEEE Transaction on Circuits and SystemsI, vol. 54, no. 5, pp. 1041-1049, 2007.
12. P.V.A. Mohan, Residue Number Systems: Theory and Applications, Springer, 2016.A.A.E. Zarandi, A.S. Molahosseini, M. Hosseinzadeh, S. Sorouri, S.F. Antão and L. Sousa, "Reverse Converter Design via Parallel-Prefix Adders: Novel Components, Methodology and Implementations," IEEE Transactions on Very Large Scale Integration (VLSI) systems, vol. 2, no. 374-378, p. 23, 2015.
13. Saikumar, K., & Rajesh, V. (2020). Coronary blockage of artery for Heart diagnosis with DT Artificial Intelligence Algorithm. International Journal of Research in Pharmaceutical Sciences, 11(1), 471-479.
14. Dr. K. Raju, Kanisetty Swathi, P. Sampath Kumar, K. Saikumar, Mr. A. Sampath Dakshina Murthym. (2020). Implementation of Low Power Cam Interface for Fault Tolerant Data Access Technique. International Journal of Advanced Science and Technology, 29(06), 3435 - 3443. Retrieved from http://sersc.org/journals/index.php/IJAST/article/view/14142.

15. Saba, S.S., Sreelakshmi, D., Sampath Kumar, P., Sai Kumar, K., Saba, S.R.(2020) Logistic regression machine learning algorithm on MRI brain image for fast and accurate diagnosis International Journal of Scientific and Technology Research. VOLUME 9, ISSUE 03, MARCH 2020.
16. Vijetha, A., Shashirekha, T., Raju, K., Rooban, S., Saikumar, K. (2020). A robust fake currency detection model using ESVM machine learning technique. Journal of Advanced Research in Dynamical and Control Systems 12(06), 170-179.
17. Raju, V & Devi, G & Sampath, A & Achanta, Sampath & Saikumar, K & Jagan, B.Omkar. (2020). HEART DISEASES CLASSIFICATION AND FEATURE EXTRACTION BY SEGMENTATION AND MACHINE LEARNING MODEL. 24. 8992-9001.
18. Aamani, Ravada & Vannala, Adinarayana & Sampath, A & Achanta, Sampath & Saikumar, K & Jagan, B.Omkar. (2020). HEART DISEASE DIAGNOSIS PROCESS USING MRI SEGMENTATION AND LASSO NET CLASSIFICATION ML. 7. 717-721. 10.31838/jcr.07.06.125.
19. Posiyya, A., Saikumar, K.(2020). Data management by librarian for academic and research perceptions. International Journal of Psychosocial Rehabilitation 24(8) 545-551.
20. Soumya, N., Kumar, K. S., Rao, K. R., Rooban, S., Kumar, P. S., & Kumar, G. N. S. 4-Bit Multiplier Design using CMOS Gates in Electric VLSI. International Journal of Recent Technology and Engineering (IJRTE) ISSN: 2277-3878, Volume-8 Issue-2, July 2019.
21. Raju, K., Pilli, S.K., Kumar, G.S.S., Saikumar, K., Jagan, B.O.L.(2019). Implementation of natural random forest machine learning methods on multi spectral image compression, Journal of Critical Reviews6(5), pp. 265-273
22. A.S. Molahosseini, A.A.E. Zarandi, P. Martins, and L. Sousa, “A Multifunctional Unit for Designing Efficient RNS-based Datapaths,” IEEE Access, accepted, 2017.
23. S.J. Piestrak, "A high speed realization of a residue to binary converter," IEEE Transactions on Circuits and Systems-II, vol. 42, pp. 661-663, 1995.
24. J.L. Beuchat, “Some modular adders and multipliers for field programmable gate arrays,” In Proc. ofIEEE International Symposium on Parallel and Distributed Processing, 2003.
25. R. Zimmermann, "Efficient VLSI implementation of modulo 2n ±1 addition and multications," in Proc.of IEEE Symposium on Computer Arithmetic (ARITH), 1999.
26. R.A. Patel, M. Benaissa and S. Boussakta, “Fast Parallel-Prefix Architectures for Modulo 2n -1 Addition with a Single Representation of Zero,” IEEE Trans. Computers, vol. 56, no. 11, pp. 1484-1492, 2007.