

Modification of the Barrel Register Full Adder (BRFA) for Performance of Montgomery Modular Multipliers

M. Jasmin, S. Philomina and G. Angelo Virgin

Abstract-- Power utilization and region are the two compels which confines the use of crucial open cryptosystem in useful gadgets. This paper proposes a plan for RSA framework which is accomplished by rehashed secluded augmentations on substantial numbers. Fast Montgomery particular duplication calculations and comparing equipment designs have a parallel prefix snake. A useful vitality calculation is utilized to diminish the vitality utilization and furthermore improve further the throughput of Montgomery measured multipliers. This engineering can sidestep the pointless parallel expansion and register to compose activities, which prompts less vitality utilization and higher performance. The alteration of the Barrel Register Full Adder (BRFA) is done as such as to apply the twofold gated clock plan procedure further decrease of vitality utilization of capacity components in BRFA.

Index Terms— Parallel Prefix Addition, Energy-efficient Architecture, Gated Clock, Montgomery Modular Multiplier, Rivest, Shamir and Adleman (RSA) cryptosystem.

I. INTRODUCTION

As the data innovation builds up, the security of data turns out to be increasingly imperative. Open key cryptography is turning into the favored answer for data security as a result of its leeway in dissemination and the board of the keys. These days, the RSA cryptography [1] is the most generally utilized crucial open cryptography, the security of which depends on the Integer Factorization Problem (IFP). Security necessities are progressively essential for private information transmission through cell phones with Internet get to, for example, advanced mobile phones and journal PCs, which require a vitality proficient cryptosystem because of their restriction of battery control.

The essential task of the RSA mark is particular exponentiation, which can be acknowledged with measured augmentation. Montgomery [2] calculation understands the steady increase with expansion and move, making the VLSI execution of secluded augmentation conceivable.

A standout amongst the most basic records for handy gadgets is controlled utilization. The length of the operands of RSA cryptosystem might be up to 1,024-piece or even 2,048-piece to accomplish required security class. In any case, the great zone and high power utilization generally make the use of RSA cryptosystem incomprehensible for

M. Jasmin, Assistant Professor, Department of Electronics and Communication Engineering, BIST, BIHER, Bharath Institute of Higher Education & Research, Selaiyur, Chennai. E-Mail: Jasmin.ece@gmail.com

S. Philomina, Assistant Professor, Department of Electronics and Communication Engineering, BIST, BIHER, Bharath Institute of Higher Education & Research, Selaiyur, Chennai.

G. Angelo Virgin, Assistant Professor, Department of Electronics and Communication Engineering, BIST, BIHER, Bharath Institute of Higher Education & Research, Selaiyur, Chennai.

battery controlled and detached gadgets. Along these lines, low power configuration turns into the test for crucial open cryptosystem RSA in handy devices. Carry spare snake involves a more region on FPGA[4]. It needs a few procedures to decrease the zone. Parallel prefix viper supplants it.

The primary classification (e.g., [5]– [8]), the information sources and yields of the Montgomery measured increase is spoken to in twofold structure, however moderate aftereffects of particular augmentation are kept in convey spare portrayal to maintain a strategic distance from the convey spread. Be that as it may, the configuration change from the express extra representation of the last item into its parallel portrayal must be performed toward the finish of each measured increase. This change can be essentially practiced by including the convey and full terms of conveying additional description. Be that as it may, the expansion still experiences long transmit proliferation, and other circuit and time are most likely required for these transformations. The second classification (e.g., [9]– [12]) takes out rehashed yield to-enter group changes through keeping up all sources of info and returns of the Montgomery measured an increase in conveying spare structure except the last advance for getting the consequence of particular exponentiation. Notwithstanding, this suggests the number of operands in secluded duplication must be expanded with the goal that extra registers to store these operands are required.

II. EXISTING SCHEMES

A many different approaches of Montgomery modular multiplies are based on a concept of carry save adder to speed up the addition process. In the previous paper proposed by Shiann-Rong [4] revokes the certificate to speed up the process and less energy consumption.

This current framework requires a more system to decrease vitality utilization. Since a convey, spare snake possesses a more zone. Essentially transmit extra viper decreases an engendering delay at the expansion procedure. So it just accelerates the expansion procedure. Be that as it may, usage of the zone is high for conveying spare snake. It expands a more vitality utilization. It likewise needs register to store a transmit at each stage. So area and its relating vitality utilization are extended.

The rest of this paper is ordered as the following segment. Area III portrays the idea of variation radix-2 Montgomery measured duplication calculations and RSA secluded exponentiation calculations. In Section IV, we propose point by point equipment design of proposed Montgomery secluded duplication.

III. MONTGOMERY MODULAR MULTIPLICATION ALGORITHM

Let the modulus N be a k -bit odd number and an extra factor R be defined as $2^k \bmod N$, where $2^{k-1} \leq N < 2^k$. Given two integers a and b , where $a, b < N$, the N -residue of a and b with respect to R can be defined as

$$A = a \times R \pmod{N}, B = b \times R \pmod{N}. \quad (1)$$

Based on (1), the Montgomery modular product Y of A and B can be obtained as

$$Y = A \times B \times R^{-1} \pmod{N} \quad (2)$$

Where R^{-1} is the inverse of R modulo N ,

i.e., $R \times R^{-1} = 1 \pmod{N}$.

The radix-2 version of the Montgomery modular multiplication algorithm, denoted as Algorithm MM, to calculate the Montgomery modular product of A and B is shown in below Algorithm. Note that the notation X_i in

this Algorithm denotes the i th bit of X in binary representation. Moreover, the notation $X_i:j$ indicates a segment of X from the i th bit to j th bit. Since the convergence range of S in Algorithm MM is $0 \leq S < 2N/2 + 2N/4 + \dots + 2N/2^{k-1} < 2N$.

Algorithm- 1 MM: Radix-2 Montgomery Multiplication:

Inputs: A, B, N (modulus)

Output: $S[k]$

$S[0] = 0;$

for $i = 0$ to $k - 1$

{

$q_i = (S[i]0 + A_i \times B_0) \bmod 2;$

$S[i+1] = (S[i] + A_i \times B + q_i \times N) / 2;$

}

if ($S[k] \geq N$) $S[k] = S[k] - N;$

return $S[k];$

The operations during this formula are simply enforced in hardware. However, these operations are performed with full exactness operands and, during this sense, they need an intrinsic limitation. Once a hardware supported algorithm is defined for n bits, it cannot work with more bits.

IV. ENERGY-EFFICIENT HARDWARE DESIGN

This section describes the detailed design of fundamental hardware architecture of MMM42. First we see the hardware architecture algorithm after that we see the MBRFA, look-ahead unit and gated clock design technique.

Algorithm-2 MMM42: 4-to-2 RCA Modified Montgomery Multiplication

Inputs : $A1, A2, B1, B2, N2 = N + 1$ (new modulus)

Outputs : $S1[k+3], S2[k+3]$

1. ($B1, B2$) = $0 + 0 + 2B1 + 2B2;$

2. ($D1, D2$) = $B1 + B2 + N2 + 0;$

3. $S1[-1] = 0; S2[-1] = 0;$

4. $q_{\sim} = 0; A_{\sim} = 0; i = -1;$

5. while ($i \delta k + 2$) {

6. if ($A_{\sim} = 0$ and $q_{\sim} = 0$)

7. ($S1[i+1], S2[i+1]$) = ($S1[i] + S2[i] + 0 + 0$) / 2;

8. else if ($A_{\sim} = 0$ and $q_{\sim} = 1$)

9. ($S1[i+1], S2[i+1]$) = ($S1[i] + S2[i] + N2 + 0$) / 2;

10. else if ($A_{\sim} = 1$ and $q_{\sim} = 0$)

11. ($S1[i+1], S2[i+1]$) = ($S1[i] + S2[i] + B1 + B2$) / 2;

12. else if ($A_{\sim} = 1$ and $q_{\sim} = 1$)

13. ($S1[i+1], S2[i+1]$) = ($S1[i] + S2[i] + D1 + D2$) / 2;

14. compute $q_{i+1}, q_{i+2}, A_{i+1}, A_{i+2}$, and bypass $i+1$;

15. if (bypass $i+1$ = 1){

16. $q_{\sim} = q_{i+2}; A_{\sim} = A_{i+2}; i = i + 2;$

17. $S1[i+1] = S1[i+1]/2; S2[i+1] = S2[i+1]/2;$

18. }

19. else{

20. $q_{\sim} = q_{i+1}; A_{\sim} = A_{i+1}; i = i + 1;$

21. }

22. }

23. return $S1[k+3], S2[k+3];$

A. MODIFIED BRFA AND LOOK-AHEAD UNIT (LU)

From an Algorithm-2 MMM42, Steps of 15– 21, \tilde{q} and \tilde{A} must be produced and put away at the i th emphasis as indicated by a bypass_{i+1} flag with the goal that they can be utilized to choose the right information operands of four-to-two to convey additional expansion at the following clock cycle. Notwithstanding, A_{i+1} and A_{i+2} are expected to deliver. The altered barrel register full viper appears on a Fig.1 utilizes two move registers RA1 and RA2 with two full adders to produce A_{i+1} and A_{i+2} at a similar clock cycle.

After A_{i+1} and A_{i+2} are gotten, a LU portrayed in Fig.2 is created to produce the bypass_{i+1} flag, \tilde{q} , and \tilde{A} . The LU comprises of an XOR entryway, a NOR door, and two two to-1 multiplexers. It creates the q_{i+1} , q_{i+2} , and bypass_{i+1} flag.

$$q_{i+1} = S1' [i]_1 = S1[i]_1 \oplus S2[i]_1 \oplus w_1.$$

$$\text{bypass}_{i+1} = \sim (q_{i+1} \vee A_{i+1}) = \sim (S1'[i]_1 \vee A_{i+1})$$

$$= \sim ((S1[i]_1 \oplus S2[i]_1 \oplus w_1) \vee A_{i+1})$$

$$q_{i+2} = S1[i + 1]_1 = S1' [i]_2 \oplus S2' [i]_1$$

Based on above formula q and \tilde{A} can be determined at the i th iteration as follows:

$$\tilde{q} = \begin{cases} q_{i+2}, & \text{if } \text{bypass}_{i+1} = 1 \\ q_{i+1}, & \text{otherwise} \end{cases}$$

$$\tilde{A} = \begin{cases} A_{i+2}, & \text{if } \text{bypass}_{i+1} = 1 \\ A_{i+1}, & \text{otherwise.} \end{cases}$$

Additionally, the bypass_{i+1} signal must be sent back to the MBRFA to determine the carry value that should be stored to FF and the bit number that registers RA1 and RA2 must be right shifted. If $\text{bypass}_{i+1} = 1$, carry_{i+2} is stored to FF and registers RA1 and RA2 are right shifted by two bit positions. Otherwise, carry_{i+1} is stored to FF and registers RA1 and RA2 are right shifted by one bit position.

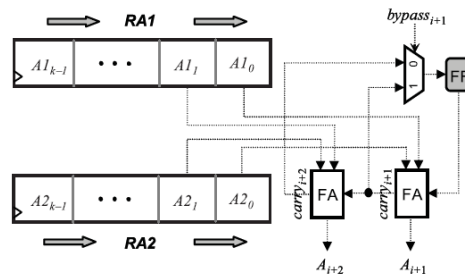


Fig-1 Modified BRFA

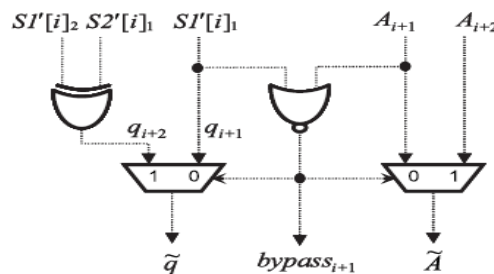


Fig-2 Look-Ahead Unit (LU)

B.Architecture of Mmm42 Multiplier

Notwithstanding MBRFA and LU, the primary part is the four-to-two RCA design. It is first used to pre-process the four-to-two convey additional increases in stage 1 and stage 2 of Algorithm-2 MMM42 through setting \tilde{A} , \tilde{q} , and registers to legitimate qualities. The delivered $(B1, B2)$ are put away to registers RB1 and RB2, and $(D1, D2)$ are put away to registers RD1 and RD2, individually. While doing the calculation of emphasis I for $-1 \leq I \leq k + 2$, the four-to-two RCA design chooses the correct wand through multiplexers M1 and M2 by utilizing \tilde{A} and \tilde{q} created at the past clock cycle. Likewise, the middle of the road esteems $S1_{[i]1}$, $S2_{[i]1}$, and $S1_{[i]2}$ created by RCA1 of the four-to-two RCA design together with the A_{i+1} and A_{i+2} delivered by MBRFA are sent to LU to produce the $bypass_{i+1}$ flag and the estimations of \tilde{q} and \tilde{A} for the following clock cycle.

The yields $S1_{[i+1]}$ and $S2_{[i+1]}$ of four-to-two RCA engineering must be partitioned by two as appeared in the means 6– 13 of Algorithm 2. We store the $bypass_{i+1}$ flag to FF and addition multiplexers M3 and M4 at the front of RCA1 as appeared in Fig.3. Thus, the right-move one-piece or no good activity will be performed at the following clock cycle as indicated by the $bypass_{i+1}$ flag put away in FF. As such, the glitches of the $bypass_{i+1}$ flag, which presumably causes superfluous unique power utilization will be obstructed by FF and not be spread to M3, M4, and RCA.

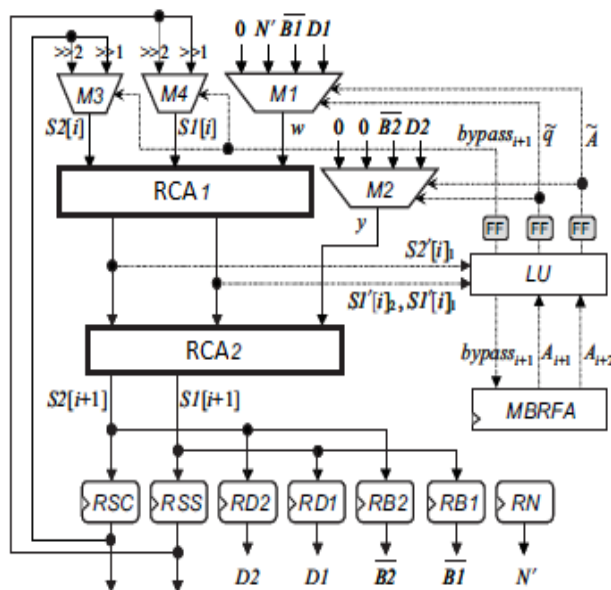


Fig-3 Block diagram for proposed MMM42 multiplier

C. Gated clock design technique

MMM42 multiplier requires a several register to store the input and output values to achieve higher performance. These registers will consume a significant portion of energy in MMM42 multiplier. Therefore, the gated clock design technique can be directly applied to these registers to reduce their area and power consumption. This multiplier with clock gating applied to RB1, RB2, RD1, RD2, and RN registers is denoted as MMM42_C1 multiplier. However, MBRFA still consumes a significant portion of power/energy and the clock gating technique cannot be directly applied to reduce its power/energy consumption since RA1 and RA2 registers must be right shifted by one or two bit positions at each clock cycle.

V. EXPERIMENTAL RESULTS

The multifaceted territory nature and primary way postponement of MMM42 and different past Montgomery multipliers can be evaluated by utilizing the convey spare snake. Notwithstanding multifaceted zone nature and primary way delay, the quantity of required clock cycles is used to decrease control utilization. In this proposed paper supplant the convey spare viper by utilizing swell send snake. Swell convey viper devours less region than contrasted with carrying an additional snake. So it uses less vitality utilization. These qualities are given in Table I.

The execution results, including the equipment zone (Area), the primary way (Delay), and power utilization (Power), which are the outcome from finished activities, the vitality utilization (Energy), region and postponement the of these secluded multipliers are given in Table II.

TABLE- I

POWER SUPPLY SUMMERY			
	Total power	Dynamic power	Static power
Power Supply (nw)	27.36	0.00	27.36

VI. CONCLUSION

Multiplied result is added with Ripple carry adder, which utilizes a less area. It reduces energy consumption and also enhances the throughput of multiplier. Moreover, the modified BRFA and adopted gated clock design technique are used FOR further reduction of the energy consumption of Montgomery modular multipliers. After that the superfluous bypassing operation is used for further reducing the energy consumption and enhance the throughput of modular multiplication.

TABLE- II
 GENERIC OUTPUT OF POWER, AREA AND DELAY FOR PROPOSED SYSTEM

Generic output	Values
Power consumption (mW)	27.36
Area (μm^2)	33%
Delay (ns)	7.508ns

REFERENCES

- [1] Rajesh E., Sankari L., Malathi L., Krupaa J.R., Naturally occurring products in cancer therapy, Journal of Pharmacy and Bioallied Sciences, V-7, PP:S181-S183, 2015.
- [2] Vanangamudi S., Prabhakar S., Thamotharan C., Anbazhagan R., Dual fuel hybrid bike, Middle - East Journal of Scientific Research, V-20, I-12, PP:1819-1822, 2014.
- [3] Brindha G., Krishnakumar T., Vijayalatha S., Emerging trends in tele-medicine in rural healthcare, International Journal of Pharmacy and Technology, V-7, I-2, PP:8986-8991, 2015.
- [4] Sharmila S., Jeyanthi Rebecca L., Naveen Chandran P., Kowsalya E., Dutta H., Ray S., Kripanand N.R., Extraction of biofuel from seaweed and analyse its engine performance, International Journal of Pharmacy and Technology, V-7, I-2, PP:8870-8875, 2015.
- [5] Thooyamani K.P., Khanaa V., Udayakumar R., Using integrated circuits with low power multi bit flip-flops in different approach, Middle - East Journal of Scientific Research, V-20, I-12, PP:2586-2593, 2014.

- [6] Jeyanthi Rebecca L., Sharmila S., Das M.P., Seshiah C., Extraction and purification of carotenoids from vegetables, *Journal of Chemical and Pharmaceutical Research*, V-6, I-4, PP:594-598, 2014.
- [7] Udayakumar R., Khanaa V., Saravanan T., Saritha G., Retinal image analysis using curvelet transform and multistructure elements morphology by reconstruction, *Middle - East Journal of Scientific Research*, V-16, I-12, PP:1781-1785, 2013.
- [8] Karthik B., Kiran Kumar T.V.U., EMI developed test methodologies for short duration noises, *Indian Journal of Science and Technology*, V-6, I-SUPPL5, PP:4615-4619, 2013.
- [9] Bomila R., Srinivasan S., Gunasekaran S., Manikandan A., Enhanced photocatalytic degradation of methylene blue dye, opto-magnetic and antibacterial behaviour of pure and la-doped ZnO nanoparticles, *Journal of Superconductivity and Novel Magnetism*, V-31, I-3, PP:855-864, 2018.
- [10] Manikandan A., Mani M.P., Jaganathan S.K., Rajasekar R., Jagannath M., Formation of functional nanofibrous electrospun polyurethane and murivenna oil with improved haemocompatibility for wound healing, *Polymer Testing*, V-61, PP:106-113, 2017.
- [11] Saravanan T., Sundar Raj M., Gopalakrishnan K., Comparative performance evaluation of some fuzzy and classical edge operators, *Middle - East Journal of Scientific Research*, V-20, I-12, PP:2633-2633, 2014.
- [12] Karthik B., Kiran Kumar T.V.U., Authentication verification and remote digital signing based on embedded arm (LPC2378) platform, *Middle - East Journal of Scientific Research*, V-20, I-12, PP:2341-2345, 2014.
- [13] Gopalakrishnan K., Sundar Raj M., Saravanan T., Multilevel inverter topologies for high-power applications, *Middle - East Journal of Scientific Research*, V-20, I-12, PP:1950-1956, 2014.
- [14] Sakthipriya N., An effective method for crop monitoring using wireless sensor network, *Middle - East Journal of Scientific Research*, V-20, I-9, PP:1127-1132, 2014.
- [15] Vijayaragavan S.P., Karthik B., Kiran Kumar T.V.U., Effective routing technique based on decision logic for open faults in fpgas interconnects, *Middle - East Journal of Scientific Research*, V-20, I-7, PP:808-811, 2014.
- [16] Kanniga E., Selvamaratham K., Sundararajan M., Kandigital bike operating system, *Middle - East Journal of Scientific Research*, V-20, I-6, PP:685-688, 2014.
- [17] Sundararajan M., Optical instrument for correlative analysis of human ECG and breathing signal, *International Journal of Biomedical Engineering and Technology*, V-6, I-4, PP:350-362, 2011.
- [18] Khanaa V., Thooyamani K.P., Saravanan T., Simulation of an all optical full adder using optical switch, *Indian Journal of Science and Technology*, V-6, I-SUPPL.6, PP:4733-4736, 2013.
- [19] Slimani Y., Baykal A., Amir M., Tashkandi N., Güngüneş H., Guner S., El Sayed H.S., Aldakheel F., Saleh T.A., Manikandan A., Substitution effect of Cr 3+ on hyperfine interactions, magnetic and optical properties of Sr-hexaferrites, *Ceramics International*, V-44, I-13, PP:15995-16004, 2018.
- [20] Suguna S., Shankar S., Jaganathan S.K., Manikandan A., Novel Synthesis of Spinel $Mn_x Co_{1-x} Al_2 O_4$ ($x = 0.0$ to 1.0) Nanocatalysts: Effect of Mn 2+ Doping on Structural, Morphological, and Opto-Magnetic Properties, *Journal of Superconductivity and Novel Magnetism*, V-30, I-3, PP:691-699, 2017.
- [21] Mathubala G., Manikandan A., Arul Antony S., Ramar P., Enhanced photocatalytic activity of spinel $Cu_x Mn_{1-x} Fe_2 O_4$ nanocatalysts for the degradation of methylene blue dye and opto-magnetic properties, *Nanoscience and Nanotechnology Letters*, V-8, I-5, PP:375-381, 2016.
- [22] Kumaravel A., Dutta P., Application of Pca for context selection for collaborative filtering, *Middle - East Journal of Scientific Research*, V-20, I-1, PP:88-93, 2014.
- [23] Krishnamoorthy P., Jayalakshmi T., Preparation, characterization and synthesis of silver nanoparticles by using phyllanthusniruri for the antimicrobial activity and cytotoxic effects, *Journal of Chemical and Pharmaceutical Research*, V-4, I-11, PP:4783-4794, 2012.
- [24] Amir M., Gungunes H., Slimani Y., Tashkandi N., El Sayed H.S., Aldakheel F., Sertkol M., Sozeri H., Manikandan A., Ercan I., Baykal A., Mössbauer Studies and Magnetic Properties of Cubic $CuFe_2 O_4$ Nanoparticles, *Journal of Superconductivity and Novel Magnetism*, V-32, I-3, PP:557-564, 2019.
- [25] Raj M.S., Saravanan T., Srinivasan V., A modified direct torque control of induction motor using space vector modulation technique, *Middle - East Journal of Scientific Research*, V-20, I-11, PP:1572-1574, 2014.
- [26] Khanaa V., Thooyamani K.P., Using triangular shaped stepped impedance resonators design of compact microstrip quad-band, *Middle - East Journal of Scientific Research*, V-18, I-12, PP:1842-1844, 2013.
- [27] Asiri S., Sertkol M., Güngüneş H., Amir M., Manikandan A., Ercan I., Baykal A., The Temperature Effect on Magnetic Properties of $NiFe_2 O_4$ Nanoparticles, *Journal of Inorganic and Organometallic Polymers and Materials*, V-28, I-4, PP:1587-1597, 2018. Thaya R., Malaikozhundan B., Vijayakumar S., Sivakamavalli J., Jeyasekar R., Shanthi S., Vaseeharan B., Ramasamy P., Sonawane A., Chitosan coated Ag/ZnO

- nanocomposite and their antibiofilm, antifungal and cytotoxic effects on murine macrophages, *Microbial Pathogenesis*, V-100, PP:124-132, 2016.
- [28] Kolanthai E., Ganesan K., Epple M., Kalkura S.N., Synthesis of nanosized hydroxyapatite/agarose powders for bone filler and drug delivery application, *Materials Today Communications*, V-8, PP:31-40, 2016.
- [29] Thilagavathi P., Manikandan A., Sujatha S., Jaganathan S.K., Antony S.A., Sol-gel synthesis and characterization studies of NiMoO₄ nanostructures for photocatalytic degradation of methylene blue dye, *Nanoscience and Nanotechnology Letters*, V-8, I-5, PP:438-443, 2016.
- [30] Thamothisaran C., Prabhakar S., Vanangamudi S., Anbazhagan R., Anti-lock braking system in two wheelers, *Middle - East Journal of Scientific Research*, V-20, I-12, PP:2274-2278, 2014.
- [31] Thamothisaran C., Prabhakar S., Vanangamudi S., Anbazhagan R., Coomarasamy C., Hydraulic rear drum brake system in two wheeler, *Middle - East Journal of Scientific Research*, V-20, I-12, PP:1826-1833, 2014.
- [32] Vanangamudi S., Prabhakar S., Thamothisaran C., Anbazhagan R., Collision control system in cars, *Middle - East Journal of Scientific Research*, V-20, I-12, PP:1799-1809, 2014.
- [33] Vanangamudi S., Prabhakar S., Thamothisaran C., Anbazhagan R., Drive shaft mechanism in motor cycle, *Middle - East Journal of Scientific Research*, V-20, I-12, PP:1810-1815, 2014.
- [34] Anbazhagan R., Prabhakar S., Vanangamudi S., Thamothisaran C., Electromagnetic engine, *Middle - East Journal of Scientific Research*, V-20, I-3, PP:385-387, 2014.
- [35] Kalaiselvi V.S., Prabhu K., Ramesh M., Venkatesan V., The association of serum osteocalcin with the bone mineral density in post menopausal women, *Journal of Clinical and Diagnostic Research*, V-7, I-5, PP:814-816, 2013.
- [36] Kalaiselvi V.S., Saikumar P., Prabhu K., Prashanth Krishna G., The anti Mullerian hormone-a novel marker for assessing the ovarian reserve in women with regular menstrual cycles, *Journal of Clinical and Diagnostic Research*, V-6, I-10, PP:1636-1639, 2012.
- [37] Thanigai Arul K., Manikandan E., Lachchumananandasivam R., Maaza M., Novel polyvinyl alcohol polymer based nanostructure with ferrites co-doped with nickel and cobalt ions for magneto-sensor application, *Polymer International*, V-65, I-12, PP:1482-1485, 2016.
- [38] Das M.P., Kumar S., An approach to low-density polyethylene biodegradation by *Bacillus amyloliquefaciens*, *3 Biotech*, V-5, I-1, PP:81-86, 2015.
- [39] Vanangamudi S., Prabhakar S., Thamothisaran C., Anbazhagan R., Turbo charger in two wheeler engine, *Middle - East Journal of Scientific Research*, V-20, I-12, PP:1841-1847, 2014.
- [40] Vanangamudi S., Prabhakar S., Thamothisaran C., Anbazhagan R., Design and calculation with fabrication of an aero hydraulic clutch, *Middle - East Journal of Scientific Research*, V-20, I-12, PP:1796-1798, 2014.
- [41] Zain, Z. (2019). High Speed and Low Power GDI based Full Adder. *Journal of VLSI Circuits and Systems*, 1(1), 5-9.
- [42] Udapa, P., & Vishwakarma, S. (2016). A Survey of MRI Segmentation Techniques for Brain Tumor Studies. *Bonfring International Journal of Advances in Image Processing*, 6(3), 22-27.
- [43] Jacob, L., & Quinn, S. (2018). Finding of Frequent Itemset with Two Mask Searches. *Journal of Computational Information Systems*, 14(2), 36-43.
- [44] Manjula, S., & Dr. Banu, R., (2014). An Efficient Compound Scoring Gene Selection Technique (CSGS) for Cancer Classification using Microarrays. *International Journal of Advances in Engineering and Emerging Technology*, 5(5), 234-247.
- [45] Saravanan, G., and Dr. Gopalakrishnan, V. (2014). Resource Allocation for Multimedia Communication on Grid Computing Environment using Hybrid ABC. *Excel International Journal of Technology, Engineering and Management*, 1(2), 36-41.
- [46] Dr. John, E.T., Skaria, B., & Shajan, P.X. (2016). An Overview of Web Content Mining Tools. *Bonfring International Journal of Data Mining*, 6(1), 01-03.
- [47] Alviri, F., & Habibi, S.F. (2015). Reviewing Self-Adaptation Frameworks for the Implementation of Enterprise Resource Planning Systems. *International Academic Journal of Innovative Research*, 2(4), 1-10.
- [48] Soni, K., Kumar, U., & Dosodia, P. (2014). A Various Biometric Application for Authentication and Identification. *International Journal of Communication and Computer Technologies*, 2(1), 6-10.
- [49] Dr. Sebasthirani, K., and Mahalingam, G. (2018). Design of Shunt Active Power Filter with Fuzzy Logic Control for Mitigating Harmonics. *Bonfring International Journal of Industrial Engineering and Management Science*, 8(2), 26-30.
- [50] Asgarnezhad, R., & Mohebbi, K. (2015). A Comparative Classification of Approaches and Applications in Opinion Mining. *International Academic Journal of Science and Engineering*, 2(5), 1-13.