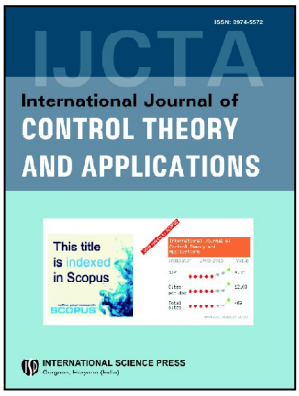


International Journal of Control Theory and Applications

ISSN : 0974-5572

Volume 10 • Number 10 • 2017

Efficient Reversible GVJ Gate as Half Adder & Full Adder and its Testing on Single Precision Floating Point Multiplier

S. S. Gayathri[1#], D. Vijayalakshmi[1*], Diana Emerald Aasha[2] and Maria Dominic Savio[3]

Department of ECE, SRM University, Chennai, Tamilnadu
E-mails: [1#]gayathri.su@gmail.com, [1]Vijayalakshmid17@gmail.com, [2]dianaemeralaasha.s@ktr.srmuniv.ac.in, [3]dom9994076650@gmail.com*

Abstract: The objective is to design a new reversible logic gate named as GVJ gate. The proposed GVJ gate can work as a half adder, Full adder by controlling the constant inputs. The researchers are now focused towards developing a system which could dissipate less power. This problem can be minimized if the circuits are constructed with reversible logic gates. With the proposed GVJ gate we have tested the working of an 8 bit adder and a single precision floating point multiplier. The performance analysis of 8 bit adder is done and compared with the existing reversible TSG gate in terms of garbage output, quantum cost; path delay and the area occupied by the 8 bit adder. From the comparison results it is clear that the proposed GVJ gate is better in all it terms stated in comparison result. .The proposed GVJ gate can be implemented on any type of adder circuits, ALU circuits, security algorithms which helps to prevent power analysis attack.

Keywords: Reversible logic, TSG gate, GVJ gate, Reversible adder

I. INTRODUCTION

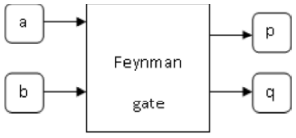
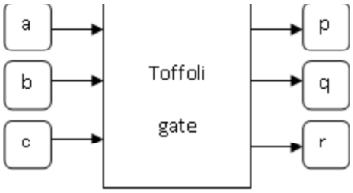
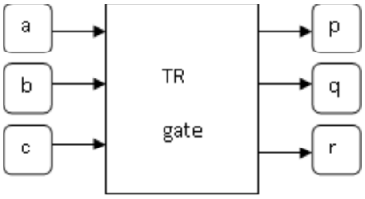
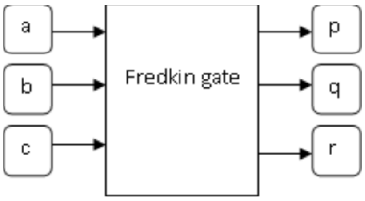
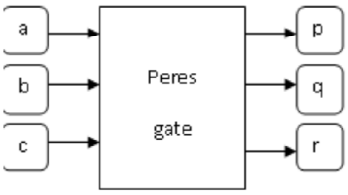
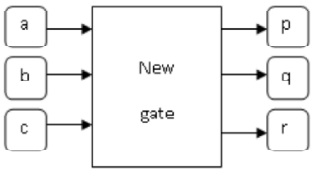
According to R.Landauer's research in the early 1960s, one bit causes an information loss. He proved power dissipation occurs due to the use of conventional irreversible logic gates. The amount of energy dissipated for every irreversible bit operation is given by kT ln2, where T is the absolute temperature, and k is Boltzmann's constant [1]. Bennett addressed this problem with a solution that if the computations are performed in reversible way, it is possible to avoid the energy dissipation [2]. Power dissipation can be minimized by constructing circuits from reversible logic gates. A logic circuit constructed with reversible logic is expected to have minimum number of reversible logic gates, garbage outputs and constant inputs to function efficiently [3].

Side Channel attacks against cryptographic systems helps to understand the physical characteristics of a device. One such attack is Power Analysis attack, in which the characteristics of a system can be known with the amount of power consumed by the system itself [4, 5, 6]. The amount of power consumed will vary from device to device depending upon the instructions executed by the device while working on different algorithm, thus when an attacker directly observes the device's power consumption, it becomes easier to predict the type of

cryptographic algorithm the key size of the system [7].A novel reversible gates in quantum cellular automata was proposed for the design of adders and its application can be implemented on ALU design[8].

II. REVERSIBLE LOGIC GATE & PROPOSED GVJ GATE

Reversible logic gates are circuits in which number of inputs is e equal to number of outputs and the outputs are unique i.e, there is a one to one correspondence between input and output. Some of the basic logic gates with its logical expression are shown below,

S.no	*Name*	*Block diagram*	*Function*
1	Feynman gate		p = a q = a⊕b
2	Toffoli gate		p=a q=b r = ab⊕c
3	TR gate		p=a q = a⊕b r = ab' ⊕ c
4	Fredkin gate		p=a q = a'b ⊕ ac' R = ab ⊕ a'c
5	Peres gate		p=a q = a⊕b r = ab⊕c
6	New gate		p=a q = ab⊕c r = a'c' ⊕ b'

Reversible logic gates have equal number of inputs and unique outputs vectors. Reversible GVJ gate is proposed to implement any type of carry save adders, carry propagate adders and multiplier.

2.1. GVJ gate

The proposed GVJ gate is a 3*3 reversible gate. Whose relationship between input and output is shown in Fig. 1,

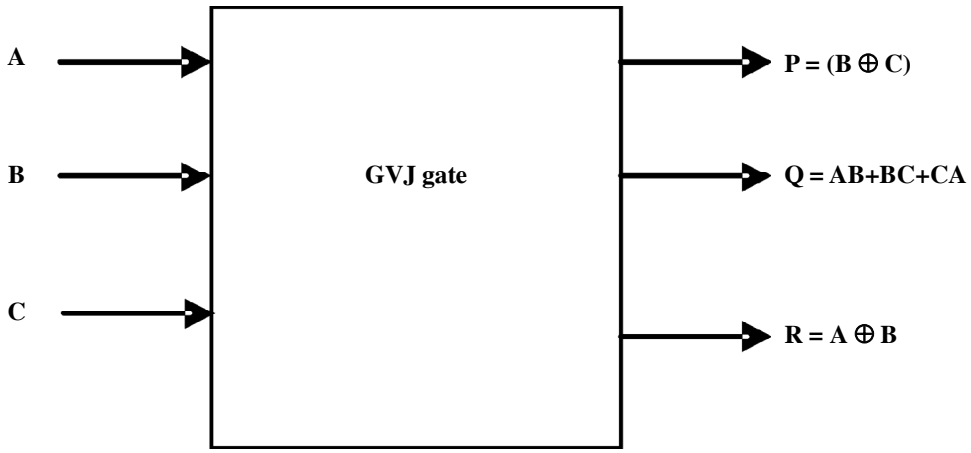


Figure 1: Reversible GVJ gate

Table 1
Truth table of GVJ gate

The truth table of the proposed GVJ gate is discussed in table 1. This table shows the bitwise relationship between the inputs and outputs of GVJ gate.

INPUTS			*OUTPUTS*		
A	*B*	*C*	*P*	*Q*	*R*
0	0	0	1	0	0
0	0	1	0	0	0
0	1	0	0	0	1
0	1	1	1	1	1
1	0	0	1	0	1
1	0	1	0	1	1
1	1	0	0	1	0
1	1	1	1	1	0

2.2. GVJ gate as half adder

GVJ gate can implement half adder logic with a garbage output.Figure.2 shows GVJ as half adder. Sum and Carry outputs are generated at the output positions of R and Q.

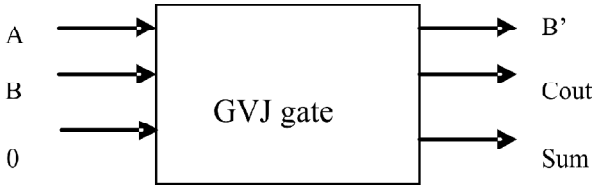


Figure 2: GVJ gate as half adder

2.3. GVJ gate as full adder

Figure 3 illustrates the working of GVJ gate as full adder.GVJ gate produces carry output and intermediate of sum output. The sum output is obtained from Feynmann gate whose input is the intermediate sum output and the third variable.

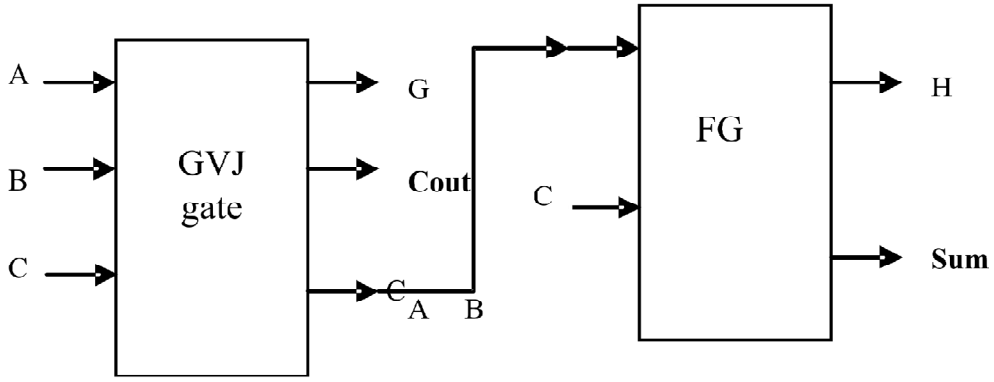


Figure 3: GVJ gate as full adder

2.4. GVJ gate as 8 bit carry propagate adder

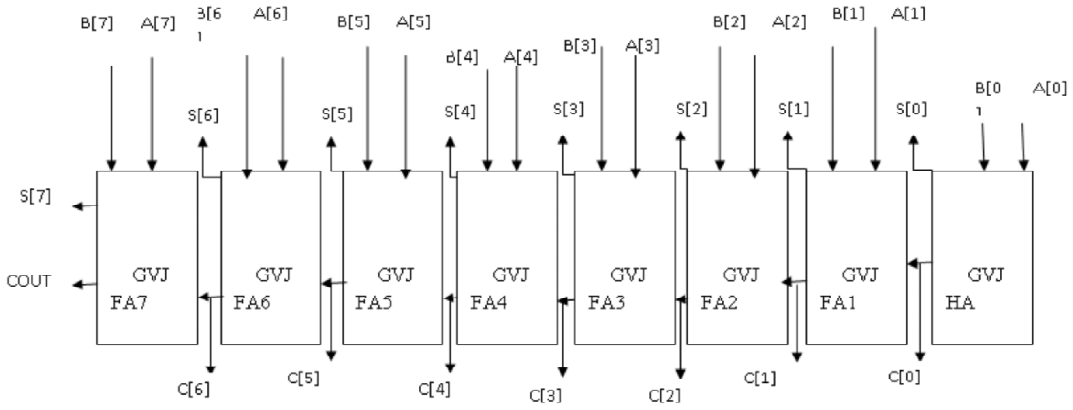


Figure 4: GVJ gate as 8 bit carry propagate adder

Figure 4 shows the 8 bit carry propagate adder realization using the proposed GVJ gate. Montgomery multiplication is the method for boosting up the speed of modular multiplication. Montgomery modular multiplier is implemented for larger operand size to design encryption and decryption algorithm for RSA security system [9].The RSA algorithm uses carry select adders and carry save adders. So the proposed adder can be implemented to any encryption technique where carry propagate adders are required.

III. TESTING OF GVJ ADDER AND MULTIPLIER ON SINGLE PRECISION FLOATING POINT MULTIPLIER

IEEE 754 floating point representations are one way of representing real number in binary form and floating point arithmetic operations are supported by all major CPU's. This work focuses on testing the working of GVJ adder and multiplier on single precision floating point (32 bits) multiplier. Figure5 shows the IEEE 754 representation of a real number by using 32 bits.

Sign (1)	Exponent (8)	Mantissa (23)

Figure 5: Single precision floating point representation

S is the sign bit of the number. Positive number is represented by '0' and negative number is represented by '1'. E is an unsigned two's-complement integer. The mantissa is an unsigned fixed point fraction with an implicit 1 to the left of the binary point.

3.1. Floating point multiplication Algorithm [10,11]

Step 1: Tentative exponent= Exponent of multiplicand+ Exponent of multiplier- Bias

Step 2: Sign out= Sign of multiplicand XOR sign of multiplier

Step 3: Mantissa out= Mantissa of multiplicand * Mantissa of multiplier

Step 4: Normalize the mantissa out by making MSB 1 by shifting the product and change the tentative exponent accordingly.

Step 5: Round or truncate the product to according to IEEE 754.

IV. SIMULATION RESULTS AND COMPARISON

4.1. Simulation result of 8 bit adder using GVJ gate

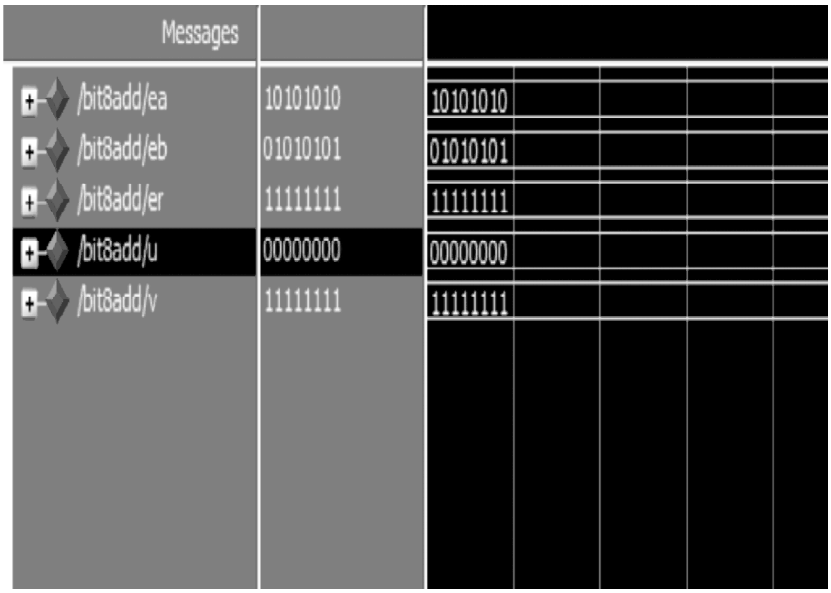


Figure 6: 8 bit GVJ adder

Figure 6 shows the simulation result of 8 bit GVJ adder. Where ea and eb are the variables assigned for 8 bit inputs and er is the result of the adder logic where the other two function u and v are the garbage outputs.

Table 2 shows the comparison between the carry propagate adder using proposed GVJ gate and existing TSG gate. Proposed GVJ structure shows less delay, garbage outputs and quantum cost and consumes less cell usage on the target device Spartan-3E XC3S1600E.

Table 2
Comparison between the proposed 8 bit adder design with GVJ gate and reversible TSG gate

Parameter	*Proposed GVJ 8Bit adder*	*TSG 8bit adder[7]*
Garbage outputs	15	16
Quantum costcost	71	104
Path delay	11.042ns	12.670ns
IOs	24	24
BELS	15	20
LUT2	1	1
LUT3	9	3
LUT4	4	11
MUX	1	1
IO BUFFERS	24	24

We have tried implementing the proposed gate design in single precision floating point multiplier. For performing the mantissa multiplication we have chosen Wallace tree multiplier.

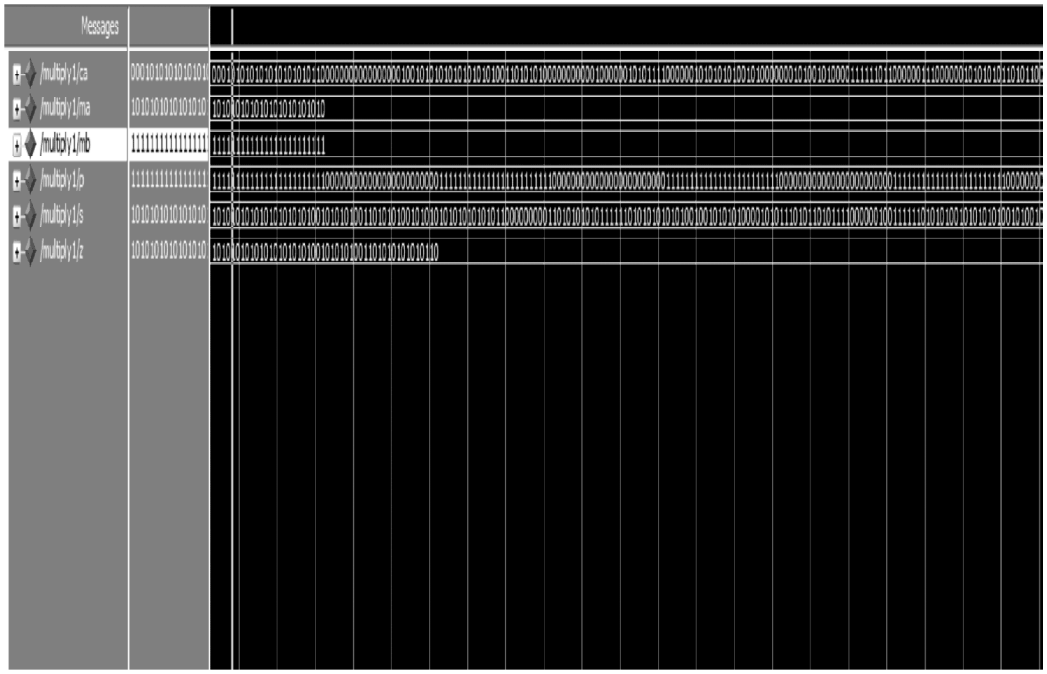


Figure 8: Simulation result for 24*24 multiplier using GVJ gate

Figure 8 shows the simulation output for the 24*24 Wallace tree multiplier structure. Here ma=101010101010101010101010 and mb=111111111111111111111111 are the two inputs and z=101010101010101010100101010100110101010101010110 is the output. Other variables are intermediate outputs.

Figure 9 shows the RTL schematic for the 24*24 multiplier using the proposed GVJ gate. The synthesis is done in Xilinx ISE with target device XC3S1600E.

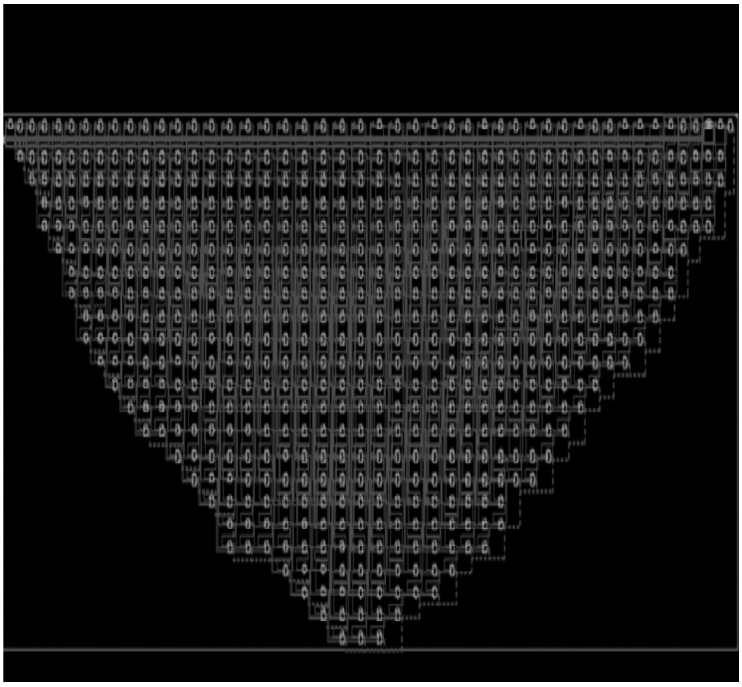


Figure 9: RTL schematic for 24*24 tree multiplier structure

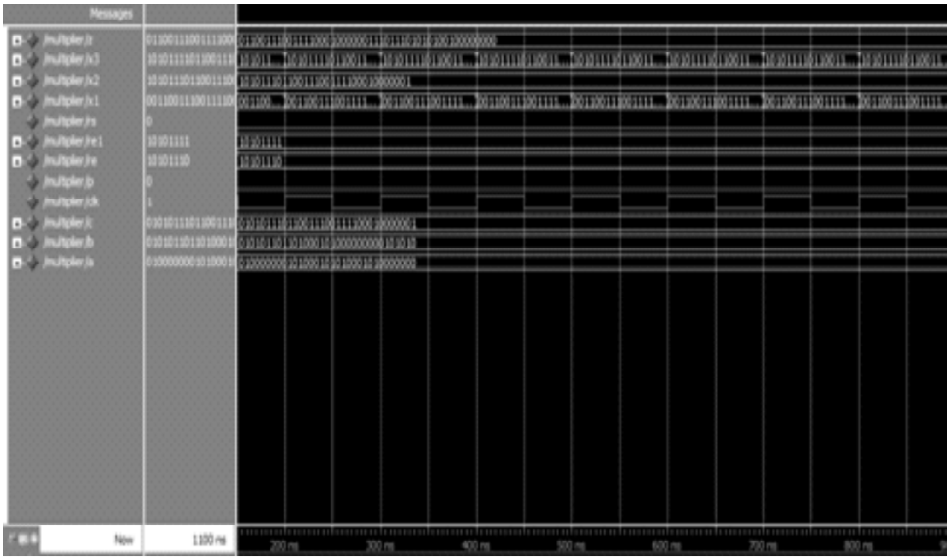


Figure 10: Simulation result for 32 bit floating point multiplier

Fig.10 shows the simulation result of the reversible single precision floating point multiplier in which a,b represents the 32 – bit input a = 01000000101000010101000101000000 and b = 01011001110100010100000000101010, The output C = 01010111011001110011110000000001

V. CONCLUSION

This paper focuses on proposing a new reversible logic gate for implementing adder circuits. The proposed reversible gate working has been tested on IEEE754 single precision floating point multiplier .As reversible

logic are power efficient, we hope that implementing hardware of cryptosystems will reduce the power analysis attack. The future direction can be extended towards implementing public key encryption techniques like RSA, using reversible logic which has a promising future in preventing power analysis attack in cryptosystems hardware.

REFERENCES

[1] R. Landauer (1961), Irreversibility and heat generation in the computing process IBM J. Research and Development 5. 183-191.

[2] C. H. Bennett (1973), Logical reversibility of computation IBM J. Research and Development 17: 525-532.

[3] M. Perkowski and P Kerntopf (2001), Reversible Logic Invited Tutorial Proc.EURO-MICRO Warsaw, Poland.

[4] I.L. Markov and D. Maslov, Uniformly switching Logic for Cryptographic Hardware, Proceedings DATE Conference, Munich, Germany, March 2005, pp. 432-433.

[5] P. Kocher, J. Jaffe, and B. Jun, Differential Power Analysis, Lecture Notes in Comp. Sci., 1666:388–397, Jan. 1999.

[6] K. Tiri and I. Verbauwhede, A Logic Level Design Methodology for a Secure DPA Resistant ASIC or FPGA Implementation, DATE 2004, pp. 246–251.

[7] Himanshu Thapliyal and Mark Zwolinsk, Reversible logic to cryptographic hardware: A new Paradigm, 49th IEEE international mid west symposium on circuits and systems, ISSN :1548-3746,pp.342-346.Aug 2006.

[8] A. Kamaraj, P. Marichamy, S. Karthika Devi, M. Nagalakshmi Subraja,"Design and Implementation of Adders using Novel Reversible Gates in Quantum Cellular Automata",Indian Journal of Science and Technology,2016 Feb, 9(8), Doi no:10.17485/ijst/2016/v9i8/87929.

[9] Ritu Gupta, Kavitha khare, Galois Field based Montgomery Multiplier for RSA Cryptosystem using Area Efficient Adder, International Journal of Computer Applications (0975 – 8887) Volume 127 – No.3,:pp.35-37October 2015.

[10] AnanthaLakshmi, A.V., Sudha, G. F.: Design of a Reversible Fused 32-Point Radix -2 Floating Point FFT Unit Using 3:2 Compressor. International Journal of New Computer Architectures and their Applications (IJNCAA) 4(4): 201-210 The Society of Digital Information and Wireless Communications, 2014 (ISSN:2220908).

[11] J. Jean Jenifer Nesam and Sivanantham Sathasivam. An Efficient Single Precision Floating Point Multiplier Architecture based on Classical Recoding Algorithm, Indian Journal of Science and Technology. 2016; Vol 9 (5): 1-7.