ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Efficient Implementation of Reversible Square Computation Using Verilog

S Srikanth, M.Tech
Assistant Professor,
MLR Institute of Technology,
Hyderabad.

Mr.S.V.S.Prasad
Associate Professor & HOD,
Department of ECE,
MLR Institute of Technology,
Hyderabad.

Saamala Sridivya
M.Tech Student,
MLR Institute of Technology,
Hyderabad.

Abstract:

Reversible computing is the emerging technology; its major role is in the field of quantum computing, optical computing, and design of low power nanocircuits. Quantum computation is modeled by quantum circuits. All the quantum operations are reversible so the quantum circuits can be built using reversible logic gates.The most frequently used computational unit for digital signal processing and multimedia applications is multiplier. To compute square of an operand, regular multipliers are used in general. This paper proposes a dedicated quantum circuit for computing square of an operand efficiently compared to the existing multipliers in the literature. The squaring unit is mathematically modeled and its metrics quantum cost, garbage outputs and ancilla input, gate count are calculated. We compared the proposed design with the existing multipliers to compute square and found that proposed square unit is efficient in terms of quantum cost, garbage outputs, ancilla inputs and gate count. The proposed reversible square circuit has 63% to 85% improvement of quantum cost, garbage outputs, ancilla inputs and gate count over existing reversible multiplier circuits.

Keywords:

Reversible logic; Arithmetic circuits; Squarer.

I. INTRODUCTION:

Reversible logic is emerging as a promising computing paradigm with applications in ultra-low power green computing and emerging nanotechnologies such as quantum computing, quantum dot cellular automata (QCA), optical computing [1, 2, 3, 8, 9, 15]. Reversible circuits are similar to conventional logic circuits except that they are built from reversible gates. In reversible gates, there is a unique, one-to- one mapping between the inputs and outputs, not the case with conventional logic.

The most promising applications of reversible logic lies in quantum computing since quantum circuit is a network of quantum gates. Each gate performs unitary operation on qubits which represents elementary unit of information. Qubits corresponds to conventional binary bits 0 and 1. Qubits are allowed to be in superposition of both the states 0 and 1. These unitary operations are reversible; hence quantum circuits are built using reversible logic gates. While designing a quantum circuitry based on reversible gates, several metrics needs to consider such as quantum cost, garbage and ancilla bits. The quantum cost of a design is the number of 1x1 and 2x2 reversible gates used in its design thus can be considered equivalent to number of transistors needed in a conventional CMOS design. The constant inputs (0 or 1) are called ancilla bits which are used in reversible circuits for storing intermediate values during computation. The garbage output refers to the output which exists in the circuit just to maintain one-to-one mapping but is not a primary or a useful output. Quantum computers of many qubits are extremely difficult to realize thus the number of ancilla inputs and the garbage outputs in the quantum circuits needs to be minimized. While designing quantum circuits one needs to optimize these parameters to improve the footprint of the overall design. Arithmetic units will be the key components of a quantum processor. Recently, researchers have concentrated their efforts towards the designs of reversible quantum adders [3, 4, 5], multipliers [6], floating point units [7], barrel shifters [12]. Among arithmetic circuits multiplier circuits play a major role to improve the performance of data processing in a processor. Squaring and cubing are the most commonly used functions in division (Newton Raphson division and Taylor series expansion), roots, or reciprocals. Squaring also finds its applications in DSP applications such as Euclidean distance computation, exponential calculation in cryptography. For powering functions like squares and cubes, a quantum circuitry of multiplier is not the most efficient solution as it results in redundant partial products and extra addition circuitry that will result in enormous overhead in terms of quantum cost, ancilla bits and garbage outputs.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Therefore, in this work we design a dedicated quantum circuitry for square computation. We are computing the square of an operand in two steps. In the first step we compute the partial products by removing the redundant ones. In the second step we reduce the number of partial products and generate the sum of partial products to give the final product term. Thereby optimizing the quantum cost, garbage outputs, gate count and ancilla inputs compared to the existing reversible quantum circuitry of multipliers. The paper is organized as follows: Section 2 presents the background on reversible logic gates; Section 3 elaborates on the design of proposed quantum circuitry for square computation; Section 4 gives the details of reversible circuit metrics calculation for n bit square unit; Sections 5 and 6 give the details of comparison and simulation results, respectively; Section 7 summarizes the conclusions.

II. REVERSIBLE LOGIC GATES :

The reversible gates used in this work are Peres gate [10], Feynman gate [14], Double Peres gate [11], and Toffoli gate [13]. Each reversible gate has a cost associated with it called quantum cost. The quantum cost of a reversible gate is the number of 1x1 and 2x2 reversible gates or quantum logic gates [11, 16] required in designing it. The quantum cost of all reversible 1x1 and 2x2 gates is taken as unity. NOT gate as shown in the Fig.1 is an example of 1x1 reversible gate.

Fig. 1. NOT gate

A.Feynman Gate (CNOT Gate):

The Feynman gate (FG) or the Controlled NOT gate (CNOT) is 2 inputs, 2 outputs reversible gate with inputs (A, B) which are mapped to outputs (P=A , Q= AB). Its quantum cost is 1. Figures 2a and 2b show the block diagram and graphical representation of the Feynman gate. The Feynman gate is widely used for either copying the signal A when B=0 thus avoiding the fan-out problem in reversible logic, or for generating the complement of the signal A when B=1.

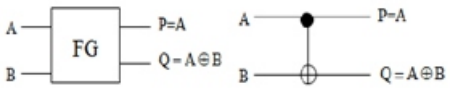

Fig. 2a. Feynman gate Fig.2b. Graphical representation

B.Peres Gate (PG):

Figures 3a and 3b show the Peres gate and its graphical representation. It is a 3*3 reversible gate having inputs (A, B, C) and outputs P = A, Q = A+B, R = AB+C. The quantum cost of Peres gate is 4 [10], since it requires 4, 2x2 reversible gates in its design.

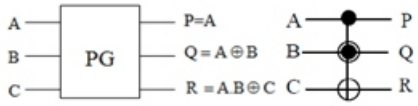

Fig. 3a. Peres gate Fig.3b. Graphical representation

C.Toffoli Gate (TG) :

Figures 4a and 4b show the Toffoli gate and its graphical representation. It is a 3*3 gate with inputs (A, B, C) and outputs P=A, Q=B, R=AB+C. Toffoli gate is one of the most popular reversible gates and its quantum cost is 5. The quantum cost of Toffoli gate is 5 [13] as it needs 5 2x2 quantum gates to implement it.

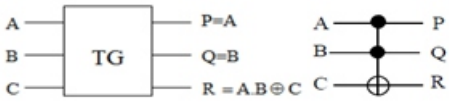

Fig.4a. Toffoli gate Fig.4b. Graphical representation

D. Double Peres Gate :

Figures 5a and 5b show the block diagram and graphical representation of the Double Peres gate (DPG), respectively. It is a 4x4 reversible gate with inputs (A, B, C, D) and outputs P=A, Q=B, R=A+B+D, S=(A+B) D+(AB+C). The quantum cost of DPG is 6 [11], as it requires 6 2x2 quantum gates to implement.

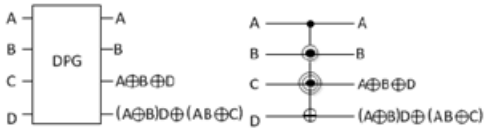

Fig. 5a. Double Peres gate Fig.5b. Graphical representation

III.PROPOSED SQUARE COMPUTATION:

In this section, we present the design of dedicated quantum circuit to compute square of an operand.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

The proposed dedicated reversible square unit incorporates the enhancement on partial product generation and summation stages. For the sake of simplicity, first we present the design of a 4x4 reversible square unit. The design of n bit square unit is presented in the next section. The partial product generation of 4 bit square unit is shown in Fig. 6. The partial product array is shown in the middle section of Fig.6, in which some of the product terms are combined using the equivalence relation

$$a_i \bullet a_j + a_j \bullet a_i = 2 \bullet a_i \bullet a_j .$$

The rectangular boxes are used to show the possible equivalence among the product terms. After applying the equivalence relation to the relevant product terms, their weight increases by 2, hence they are shown in the next column. The arrow shows the shifting of the combined terms left by one position. The final reduced partial products are shown in the last section in Fig.6.

Fig.6. Partial product generation of 4x4 square unit

A.Step 1:Partial products generation using Reversible Logic gates :

While performing square computation, the first step is to generate all partial products in reversible manner. To perform this step, we have used Toffoli gates to generate the reduced partial products as illustrated in Fig. 7. For ANDing two operands, the third input C of the Toffoli gate is connected to zero which requires one ancilla input (constant zero). The series connection of Toffoli gates gives zero garbage outputs while generating the partial products. The inputs are regenerated at the output along with the expected partial products. The basic property of the reversible logic is to preserve the input bits, hence the regenerated input bits at the output sections are not considered as garbage outputs. This is the main motivation to choose Toffoli gate over the Peres gate for ANDing the two operands.

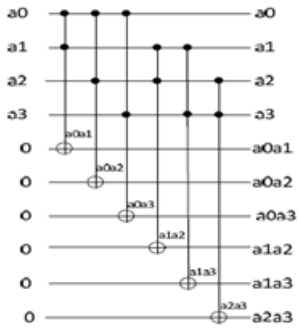

Fig. 7. Proposed reversible partial production generation circuitry for 4x4 square unit

B.Step 2: Summation of reduced partial products :

The final product terms of the proposed reversible 4x4 square unit are generated in the summation stage using carry save method as depicted in Fig. 8. The reversible full adders and half adders are the basic blocks of this architecture. The reversible full adder is designed using Double Peres gate by setting inputs C=0 and D=Cin as shown in Fig.9. Similarly, half adder is constructed using Peres gates by setting input C=0 as shown in Fig. 10. The complete reversible circuitry of 4 bit square unit using the symbols of Toffoli gate, Peres gate, and Double Peres gate is shown in Fig. 11.

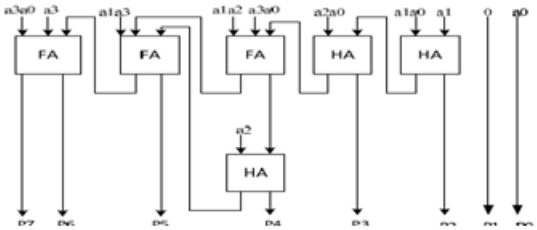

Fig.8. Summation circuitry for 4x4 square unit

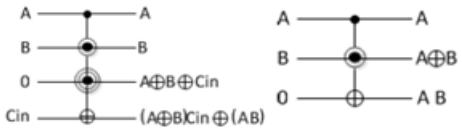

Fig. 9. DPG gate as full adder Fig. 10. Peres gate as half adder

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

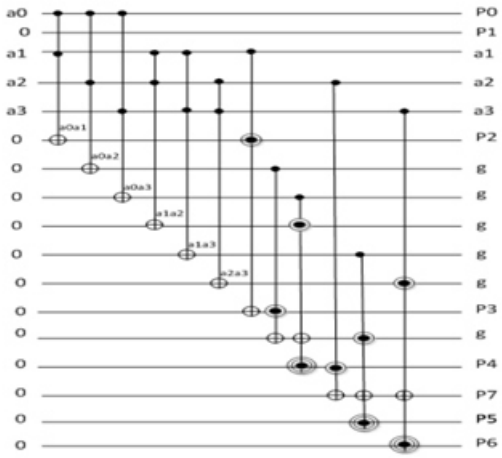

Fig. 11. Complete Reversible circuit of 4 bit square unit

IV REVERSIBLE CIRCUIT METRICSFOR SQURER:

The reversible design of 4 bit square unit (Fig. 11) can be extended to any size. In this section we present the estimation of n bit square circuit metrics such as quantum cost, ancilla inputs, and garbage outputs. For n bit square unit, the required number of partial products are generated by using the reduction method (as illustrated in Fig.6). It is computed using the generalized computation equation 1 as shown below. Here k and l indicate the bit position, and n is the number of bits used to represent the operand value. The array of partial products generated can be mathematically expressed as

$$a^2 = \sum_{k=0}^{n-1} a_k \bullet 2^{2k} + \sum_{k=0}^{n-2} \sum_{l=k+1}^{n-1} a_k \bullet a_l \bullet 2^{k+l+1} \qquad (1)$$

The estimation of circuit metrics is shown in two steps. In Step 1 only partial products generation circuit is considered and it is generalized for n bit square computation. In Step 2 the complete circuit estimation is discussed.

A. Step 1: Calculation of Circuit Metrics for Partial Product Generation The total number of partial products of the proposed design of n bit square unit is computed using equation 1a. Here PP(n) indicate the number of partial products for n bits.

$$PP(n) = \frac{\left(n^2 + n\right)}{2} \qquad (1a)$$

Partial products are generated using the Toffoli gates as illustrated in Fig 7.

As shown in Fig.7 few partial products are same as operand bits. It can be directly generated from the output of the Toffoli gate. This reduces the number of partial products need to be generated. So the number of partial products need to be generated are now reduced by number of operand bits. So equation 1a is modified as below.

$$PP(n) = \left(n^2 - n\right) /2 \qquad (1b)$$

The quantum cost of Toffoli gate is 5. The quantum cost (qcost) for n bit operand is computed as product of quantum cost of Toffoli gate and number of reduced partial products (PP(n)). It is mathematically shown in equation 2.

$$Qcost(n) = \left(5 \bullet \left(\frac{n^2 - n}{2}\right)\right) \qquad (2)$$

Since each Toffoli gate uses one ancilla bit, for n bit square computation the total number of ancilla inputs required is given by equation 3.

$$Ancilla(n) = \left(\frac{n^2 - n}{2}\right) \qquad (3)$$

B. Step 2: Calculation of Circuit Metrics for complete n bit square circuit Performance metrics such as quantum cost, ancilla input and garbage outputs are modeled mathematically for the complete circuit as shown in the equations 5a, 6a, 7a respectively. Quantum cost(Qcost) for n bit number is the sum of qcost of partial product generation circuit, qcost of total number of reversible full adders used in the summation circuit and qcost of total number of reversible half adders used in the summation circuit. The qcost of reversible full adder and reversible half adder is already discussed in Section III. The equation 5 gives better clarity for the computation of qcost.

$$Qcost(n) = \{Qcost\ of\ PP\ generation\ circuit + Quantum\ cost\ of\ Full\ Adder \bullet \left(\frac{Number\ of}{Full\ Adders}\right) + Quantum\ cost \bullet \left(\frac{number\ of}{Half\ Adders}\right)\} \qquad (5)$$

Mathematical modeling of the above expression is shown in equation 5a

$$Qcost(n) = \left(\frac{11 \bullet n^2 - 15 \bullet n + 4}{2}\right) \qquad (5a)$$

Generalized computation of ancilla inputs is given by equation 6 , mathematical modeling is given by equation 6a.

$$Ancilla\ Inputs(n) = Number\ of\ ancilla\ bits\ of\ PP\ generation\ circuit + Number\ of\ ancilla\ bits\ for\ Full\ adder \bullet \left(\frac{Number\ of}{Full\ Adders}\right) + Number\ ancilla\ bits\ for\ Half\ Adder \bullet \left(\frac{Number\ of}{Half\ Adders}\right) \qquad (6)$$

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

$$Ancilla\ Inputs(n) = \left(n^2 - n + 1\right) \quad (6a)$$

Similarly, garbage outputs equation is derived as below. Here the garbage outputs of partial products generation circuit is zero as explained in section III.

$$Garbage\ Outputs(n) = garbage\ output\ of\ PP\ generation\ circuit + garbage\ output\ bits\ produced\ by\ Full\ Adder \bullet \left(\begin{matrix}Number\ of\\ Full\ Adders\end{matrix}\right) + garbage\ output\ bits\ produced\ by\ Half\ Adder \bullet \left(\begin{matrix}Number\ of\\ Half\ Adders\end{matrix}\right) \quad (7)$$

$$Garbage\ Outputs(n) = \left(n^2 - 2 \bullet n + 1\right) \quad (7a)$$

It is observed from the calculation that gate count is one less than the ancilla (n) that is Gate Count (n)= (n2-n). Since there is one ancilla bit for each gate of the circuit, gate count is directly obtained from number of ancilla bit. We have subtracted one from the equation 6a since one ancilla bit is used for the partial product PP1 which is the constant input in the second column. For more clarity on this refer Fig.7.

V .COMPARISON AND RESULTS:

Reversible circuit metrics quantum cost, garbage bits and ancilla inputs are computed for variable bit length of an operand for the complete square unit and the same is depicted in the Fig 12.

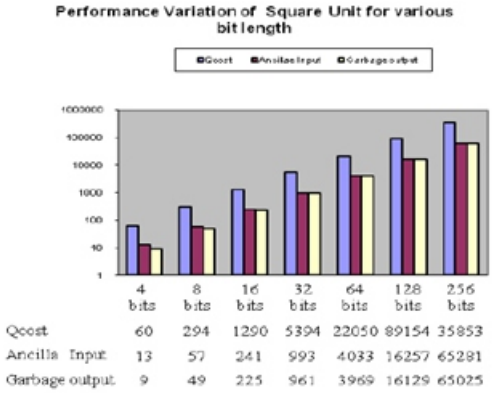

Fig. 12. Reversible circuit metrics variation for variable bit length of square

It is observed from the chart (Fig.12) that as the number of bits increases, the value of garbage outputs increases nearly with ancilla inputs. The values shown in Fig.12 are obtained by calculating quantum cost, ancilla inputs, garbage outputs using the equations 5a, 6a, 7a, respectively.

The reversible circuit metrics of partial product generation and final product term generation for 4x4 square unit are calculated and are compared with the existing multipliers in the literature. The Reversible circuit metrics comparison of partial product generation circuit for 4x4 square unit is shown in Table 1 and the performance parameter comparison of complete circuit for 4x4 square unit is shown in Table 2.

TABLE 1. Reversible circuit metrics comparison of partial product generation circuit for 4x4 square unit:

Partial product generator	CI	% IM	G O	% IM	G C	% IM	QC	% IM
Our work	06	NA	0	NA	06	NA	30	NA
Ref[6]-Design I	16	63	16	100	16	63	96	69
Ref[6]-Design II	16	63	8	100	16	63	104	71
Ref[17]	16	63	32	100	16	63	112	73
Ref [18]	16	63	8	100	16	63	100	70
Ref [19]	16	63	32	100	16	63	112	73
Ref [20]	16	63	8	100	16	63	104	71
Ref [21]	16	63	32	100	16	63	112	73
Ref [22]	16	63	32	100	16	63	112	73
Ref [23]	16	63	16	100	16	63	112	73

The notations followed in the table are CI (constant Input), %IM (percentage improvement), GO (Garbage Outputs), GC (Gate Count), QC (Quantum Cost). The values captured in the table are rounded off to its nearest digit. The maximum variation of the value is +0.5. It is observed from Table 1 that maximum of 63% improvement on constant inputs, gate count are achieved in comparison with all the work considered for comparison. For quantum Cost, minimum of 69% improvement is achieved in comparison of the work proposed in Design 1 of [6] and maximum improvement of 73% is achieved when we compared our work with the Designs proposed in [17,19]. Garbage Output improvement is 100% since our design has zero garbage output.

Table 2 shows the comparison result of complete circuit of reversible 4x4 square unit. It is observed from Table 2 that minimum 54% improvement on constant inputs is achieved in comparison with the design proposed in [6,18,21] and maximum of 83% improvement is achieved in comparison with the design in [20]. For garbage outputs minimum percentage improvement of about 63% and maximum of 85% is achieved for the work proposed in [6] respectively. In continuation with this comparison, minimum improvement of 57% is obtained on gate count for the designs [6,18] and maximum improvement of 85% for the design [20]. Finally the quantum cost improvement is of about 69% obtained for the designs in [6,18] .

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

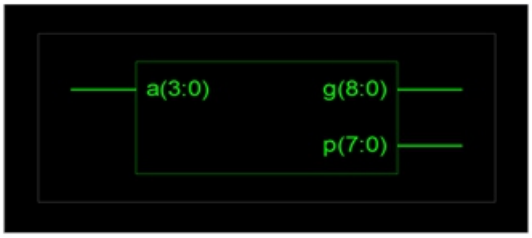

Fig 13.RTL schematics of 4x4 squarer

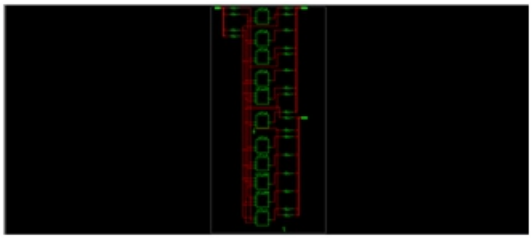

Fig 14.Technology schematics of 4x4 squarer

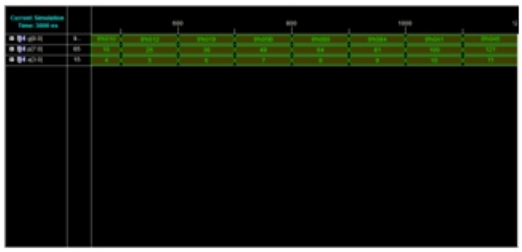

Fig 16.Simulation results of 4x4 squarer

VI.CONCLUSION:

The proposed reversible 4x4 square design is proved to be better than the existing designs in terms of the quantum cost, gate count, garbage outputs, and ancilla inputs. In the reduced partial product generation circuitry, maximum of 63% improvement is achieved for ancilla inputs and gate count; there are zero garbage outputs in the proposed circuit and 73% improvement on quantum cost. In addition to this, final product generation circuitry has maximum of 85% improvement over garbage outputs and gate count, 83% improvement on quantum cost and ancilla inputs. The square unit will find applications in reversible computing of multipliers.

REFERENCES:

[1] R. Landauer, "Irreversibility and heat generation in the computational process,"IBM J. Research and Development, vol. 5, pp. 183–191, Dec.1961.

[2]C. H. Bennett, "Logical reversibility of computation,"IBM J. Research and Development, vol. 17, pp. 525–532, Nov. 1973.

[3] V. Vedral, A. Barenco, and A. Ekert, "Quantum networks for elementary arithmetic operations," Phys. Rev. A, vol. 54, no. 1, pp. 147– 153, Jul 1996.

[4] Y. Takahashi, "Quantum arithmetic circuits: a survey," IEICE Trans. Fundamentals, vol. E92-A, no. 5, pp. 276–1283, 2010.

[5] B. S. Choi and R. Van Meter, "On the effect of quantum interaction distance on quantum addition circuits," J. Emerg. Technol. Comput. Syst., vol. 7, pp. 11:1–11:17, August 2011.

[6] M. Z. Moghadam and K. Navi, "Ultra-area-efficient reversible multiplier," Microelectronics Journal, Vol. 43, no. 6, 377-385, 2012.

[7] T. D. Nguyen, and R. Van Meter, "A Space-Efficient Design for Reversible Floating Point Adder in Quantum Computing", arXiv preprint arXiv:1306.3760, 2013.

[8] H. Thapliyal, N. Ranganathan and S.Kotiyal, "Reversible Logic Based Design and Test of Field Coupled Nanocomputing Circuits", To Appear Springer Lecture Notes on Computer Science State-of the-Art-Survey Series Special Volume on Field-Coupled Nanocomputing, 2014.

[9] H. Thapliyal, N. Ranganathan and S. Kotiyal, "Design of Testable Reversible Sequential Circuits ", IEEE Transactions on VLSI, vol. 21, no.7, pp.1201-1209, July 2013.

[10] A. Peres, "Reversible logic and quantum computers," Phys. Rev. A, Gen. Phys., vol. 32, no. 6, pp. 3266–3276, Dec. 1985.

[11] W. N. Hung, X. Song, G.Yang, J.Yang, and M. Perkowski, "Optimal synthesis of multiple output boolean functions using a set of quantum gates by symbolic reachability analysis," IEEE Trans. Computer-Aided Design, vol. 25, no. 9, pp. 1652–1663, Sept. 2006.

[12] S. Kotiyal, H. Thapliyal, and N. Ranganathan, "Design of a reversible bidirectional barrel shifter," Proceedings of the 11th IEEE NANO, Portland, Aug. 2011, pp. 463–468.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

[13] E. Fredkin and T. Toffoli, "Conservative logic," International J. Theor.Physics, vol. 21, pp. 219–253, 1982.

[14] R. Feynman, "Quantum Mechanical Computers," Optical News, pp. 11- 20, 1985.

[15] M. A. Nielsen and I. L. Chuang, Quantum Computation and Quantum Information. New York: Cambridge Univ. Press, 2000.

[16] J. A. Smolin and D. P. DiVincenzo, "Five two-bit quantum gates are sufficient to implement the quantum fredkin gate," Physical Review A, 53: pp.2855–2856, 1996.

[17] H. R. Bhagyalakshmi and M. K. Venkatesha, "An improved design of a multiplier using reversible logic gates," Int. J. Eng. Sci. Technol. 2 (8), pp. 3838–3845, 2010.

[18] M. Haghparast, M. Mohammadi, K. Navi, and M. Eshghi, "Optimized reversible multiplier circuit."Journal of Circuits, Systems & Computers, vol. 18, no. 2, pp. 311 – 323, 2009.

[19] M. Haghparast, S. Jassbi, K. Navi, and O. Hashemipour, "Design of a novel reversible multiplier circuit using HNG gate in nanotechnology,"World Applied Sciences Journal , vol. 3, no. 6, pp. 974–978, 2008.

[20] A. Banerjee and A. Pathak, "An analysis of reversible multiplier circuits", arXiv:0907.3357,pp. 1–10, 2009.

[21] M. S. Islam, M. M. Rahman, Z. Begum and M. Z. Hafiz, "Low cost quantum realization of reversible multiplier circuit," Information Technology Journal, vol. 8, no. 2, pp.208-213, 2009.