



International Journal of Advanced Research Foundation

Website: www.ijarf.com, Volume 2, Issue 8, August 2015)

Design of Dedicated Reversible Quantum Circuitry for Square Computation

Akutota Vinay Kumar
M.Tech Student (VLSI-SD)
Dept.of.ECE, GNIT
a.vinaykumara6@gmail.com

Mrs.A Swetha
Associate Professor
Dept.of.ECE, GNIT
swethavlsi@yahoo.com

Mr. M Suman Kumar
Associate Professor
Dept.of.ECE, GNIT
sumankumar.gnit@gmail.com

Prof B Kedarnath
HOD-ECE
Dept.of.ECE, GNIT
hodece.gnit@gniindia.org

Abstract— Quantum computation is modeled by quantum circuits. All the quantum operations are reversible so the quantum circuits can be built using reversible logic gates. Reversible computing is the emerging technology; its major role is in the field of quantum computing, optical computing, and design of low power nano circuits. 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; Toffoli gate.

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, 26, 28], multipliers [6, 29], floating point units [7, 30], barrel shifters [12, 27]. 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 [24, 25]. 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. 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. BACKGROUND ON 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 gates.



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= A⊕B). 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.

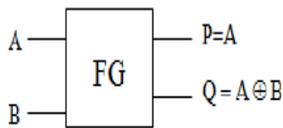


Fig. 2a. Feynman gate

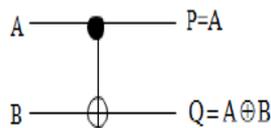


Fig.2b. Graphical representation

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.

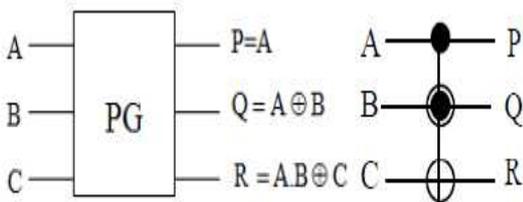


Fig. 3a. Peres gate

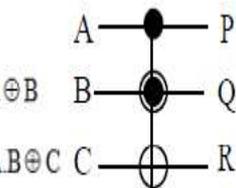


Fig.3b. Graphical representation

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.

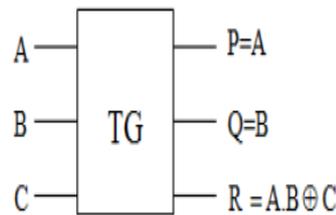


Fig.4a. Toffoli gate

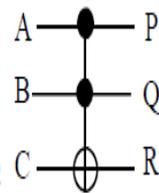


Fig.4b. Graphical representation

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.

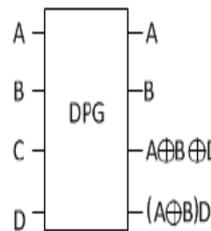


Fig. 5a. Double Peres gate

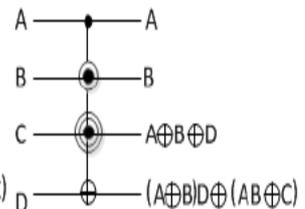


Fig.5b. Graphical representation

III. PROPOSED QUANTUM CIRCUITRY FOR SQUARE COMPUTATION

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



International Journal of Advanced Research Foundation

Website: www.ijarf.com, Volume 2, Issue 8, August 2015)

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

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

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.

$$PP(n) = \frac{(n^2 + n)}{2} \quad (1a)$$

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.

$$PP(n) = \frac{(n^2 - n)}{2} \quad (1b)$$

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.

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

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.

$$Ancilla(n) = \frac{(n^2 - n)}{2} \quad (3)$$

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.

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

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

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

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

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

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

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

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

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

It is observed from the calculation that gate count is one less than the ancilla (n) that is Gate Count (n) = (n-2)·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.

Result analysis:

RTL Top Level Output File Name : SQUARER.ngr

Top Level Output File Name : SQUARER

Output Format : NGC
Optimization Goal : Speed
Keep Hierarchy : NO

Design Statistics
IOs : 21



International Journal of Advanced Research Foundation

Website: www.ijarf.com, Volume 2, Issue 8, August 2015)

Cell Usage :

# BELS	: 12
# GND	: 1
# LUT2	: 6
# LUT3	: 2
# LUT4	: 3
# IO Buffers	: 21
# IBUF	: 4
# OBUF	: 17

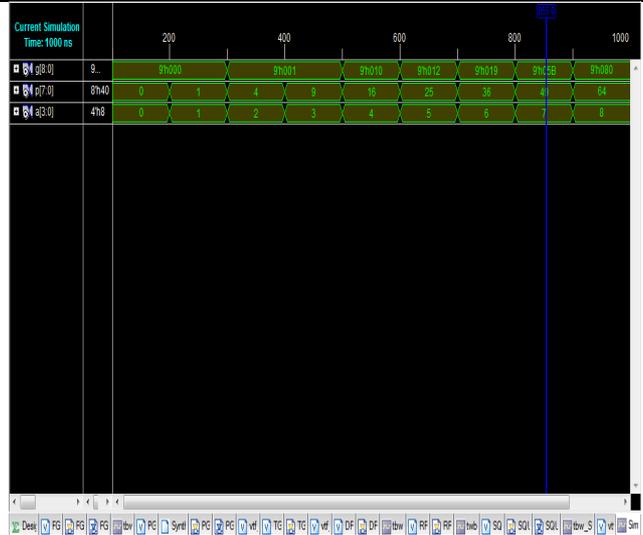
Selected Device: 3s100evq100-4

Number of Slices: 6 out of 960 0%

Number of 4 input LUTs: 11 out of 1920 0%

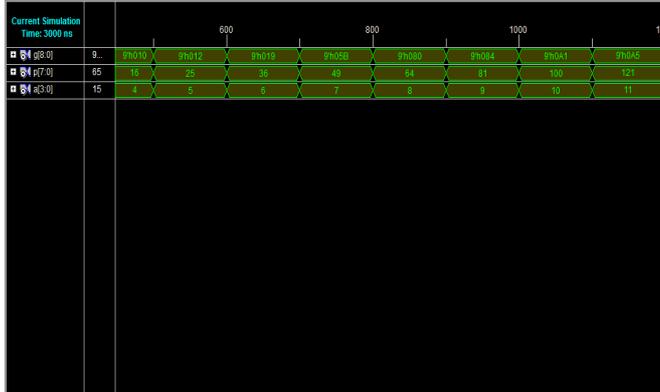
Number of IOs: 21

Number of bonded IOBs: 21 out of 66 31%

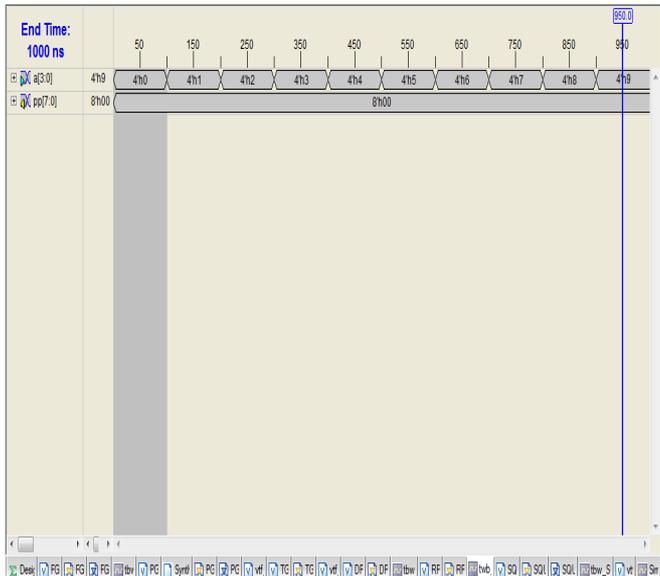


VII CONCLUSION

End module



Test bench:



In this work, we have presented efficient dedicated quantum circuit for square computation, primarily optimizing the quantum cost, gate count, garbage outputs and ancilla inputs. 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 and specially dividers like Newton Raphson divider.

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.



International Journal of Advanced Research Foundation

Website: www.ijarf.com, Volume 2, Issue 8, August 2015)

- [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.
- [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.