CSWAP GATE BASED COMBINATIONAL CIRCUITS FOR SECURE COMMUNICATION

Author[1]: TALLAM JYOTHI SAI ABHIJITH,
Author[2]: RAVELA ANUDEEP,
Author[3]: YARLAGADDA MAHESH BABU.

[1] *Student, ECE, VASIREDDY VENKATADRI INSTITUTE OF TECHNOLOGY, A.P., INDIA*
[2] *Student, ECE, VASIREDDY VENKATADRI INSTITUTE OF TECHNOLOGY, A.P., INDIA*
[3] *Student, ECE, VASIREDDY VENKATADRI INSTITUTE OF TECHNOLOGY, A.P., INDIA*

ABSTRACT

Quantum computing is an emerging technology in the present-day research and developments. It depends upon the basic physical phenomena like interference, superposition, entanglement etc. which promise an efficient solution to the complex mathematical problems that take years to solve. Reversibility is another feature in this, which allows to detect the input by observing the output. Quantum computing supports some sort of gates used to process the input data applied. Among these gates Hadamard gate is an important one that offers superposition of the input and defines all the possible inputs required to determine the output. This is a special feature which is required in the verification and testing of the VSLI designs under test. Further, these quantum gates can also be used to design arithmetic and logical circuits for the required applications and they promise higher speed. In this proposed work, Quantum gates have been defined as logic gates to design digital circuits. Also, a CSWAP gate has been used to propose the combinational circuits like Multiplexers, Demultiplexers and Decoders. These are very much helpful for the implementation of quantum entanglement to provide secure communication.

Keyword: - *Key word1*:*Quantum Computing, Key word2: CSWAP, Key word3: Entanglement, Key word4: CST- Superposition, key word5: Interference.*

1. INTRODUCTION

In High-speed computing plays a very important role in our day-to-day activities from personal to public. But it all happen at a cost of increased power consumption. Advancements in transistor technology led to the invention of Complementary Metal Oxide Semiconductor (CMOS) transistor accomplished the need of the time. However, various applications of computing technologies such as commerce, medical, governance and other logistics using CMOS still in wane due to high speed up demands. Thus, the present day computations need a substitute to the existing computing systems. Quantum computing is one among the remarkable substitutes.

Quantum computer takes leverage of basic properties of quantum mechanics to perform computations like superposition of states, interference, and entanglement. Moreover, it gets a computational advantage with crucial properties of reversibility, and each computing sub system must be reversible. These properties lead quantum computers to promise wide capabilities of quantum information processing in the areas like sensing and communication also. Quantum researchers, apart from complex computational tasks, working towards logical systems to come up with fast decision making capabilities. The basic building blocks of logic circuits are the basic logic gates, which can be realised by using quantum gates. Quantum system designers have been working over the implementations of logic circuits.These were implemented using the quantum gates theoretically with a qubit characterization. Several quantum programming software are available to design and implement the quantum circuits such as #Q, Cirq, Qiskit etc., among them #Q cannot generate quantum circuits.

2. PROPOSED WORK AND DESIGNED METHODOLOGY:

Figure Designing the multiplexers with low cost quantum gates leads to fast and low area circuits. These multiplexers can be used in the implementation of quantum entanglement which provides a secured communication between to parties. Multiplexers were designed using quantum gates such as CSWAP . The reported multiplexers which were reported theoretically consist of CSWAP gate which occupies more area. Implementation of the quantum circuits using HDL and its realization with classical logic gates with MOS transistors provides garbage outputs with ancilla. These implementations further consume more power and delay. To overcome the above mentioned limitations, multiplexers have been proposed in this work with CSWAP gates and implemented using IBM Qiskit with Python coding.

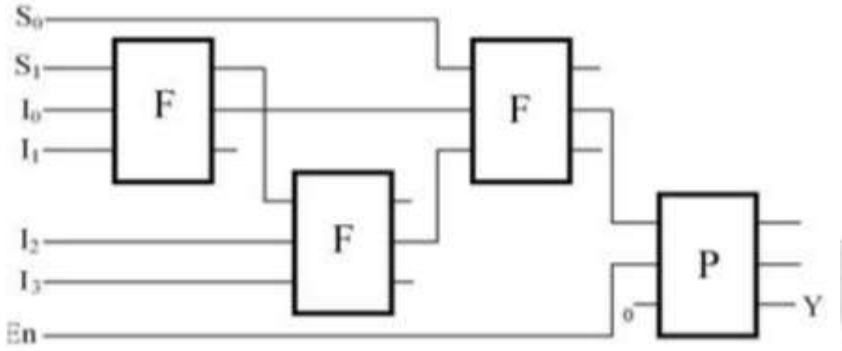

Fig. 1.1*:* Existing Design on 4:1 Multiplexer with Theoretical Implementation

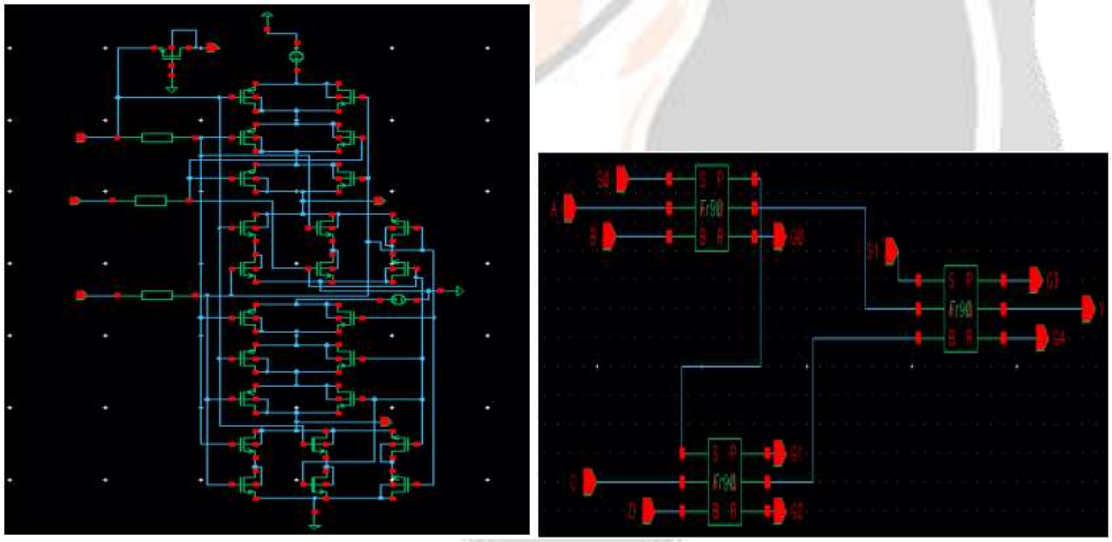

Fig. 1.2: Existing Design on 4:1 Multiplexer with HDL Implementation

In order to design arithmetic circuits with quantum gates, cascading is a process to be implemented to develop high end structures. It is implemented using *compose ()* class in Python. Further, Demultiplexers and Decoders are also proposed and realized using the same CSWAP gate.

2.1 DESIGNED METHODOLOGY

- Initially, a 2x1 multiplexer is proposed using CSWAP gate with low quantum cost and anclilla (constant input).
- Proposed 2x1 multiplexer is used to design 4x1 and 8x1 multiplexers.
- This CSWAP gate is used to develop demultiplexers and decoders.
- IBM Qiskit Simulator is used to verify the proposed design with Python Programming.

3. QUANTUM GATES

In general, quantum scientists work over the two-level qubit systems to define quantum algorithms and, in turn quantum computers. In these systems, there are two states *viz.*, |0 and |1 , and these are called to be the computational basis of the twolevel qubit system represented with vectors as follows;

These states are same as binary bits, '0' and '1' used in classical systems. But the qubit differs from the classical bit as it may also be represented as a superposition of both states |0 and |1 . In order to evolve the operations, some sort of operators are used over these states, which are in the form of matrices. There are three basic operators depend on number of inputs, and they are unary, binary and ternary. As far as the number of outputs are concerned, they are same as inputs due to reversibility. Quantum gate is represented with its operator to perform an operation over the qubits.Basically, operators and gates are interchangeably used

3.1 UNARY GATES

The Identity (I), NOT (X) and Hadamard (H) gates are represented with unary operators, whose symbols and matrix forms are illustrated below.

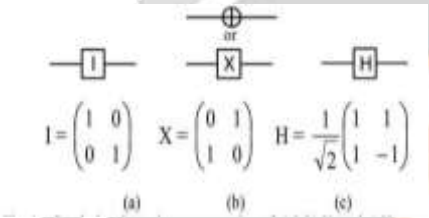

Fig.3.1. Symbol and matrix representation of a) I, b)X, and c)H gates

$$I|0\rangle = \begin{pmatrix}1&0\\0&1\end{pmatrix}\begin{pmatrix}1\\0\end{pmatrix} = \begin{pmatrix}1\\0\end{pmatrix} = |0\rangle \text{ and}$$

$$I|1\rangle = \begin{pmatrix}1&0\\0&1\end{pmatrix}\begin{pmatrix}0\\1\end{pmatrix} = \begin{pmatrix}0\\1\end{pmatrix} = |1\rangle$$

Fig.3.2. Operation of IDENTITY gate

$$X|0\rangle = \begin{pmatrix}0&1\\1&0\end{pmatrix}\begin{pmatrix}1\\0\end{pmatrix} = \begin{pmatrix}0\\1\end{pmatrix} = |1\rangle \text{ and}$$

$$X|1\rangle = \begin{pmatrix}0&1\\1&0\end{pmatrix}\begin{pmatrix}0\\1\end{pmatrix} = \begin{pmatrix}1\\0\end{pmatrix} = |0\rangle$$

Fig.3.3. Operation of NOT gate

$$H|0\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix}1&1\\1&-1\end{pmatrix}\begin{pmatrix}1\\0\end{pmatrix} = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\1\end{pmatrix} = \frac{|0\rangle + |1\rangle}{\sqrt{2}} \text{ and}$$

$$H|1\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix}1&1\\1&-1\end{pmatrix}\begin{pmatrix}0\\1\end{pmatrix} = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\-1\end{pmatrix} = \frac{|0\rangle - |1\rangle}{\sqrt{2}}$$

Fig.3.4. Operation of HADAMARD gate

Controlled SWAP gate is abbreviated as CSWAP as it swaps the values of B and C at the output when A = 1. Also, it can be used as OR gate to produce A + B at the middle output when C = 1 and as an AND gate to produce AB at the bottom output when C =1. This gate is also known as Fredkin Gate. Also, in CCNOT and CSWAP gates, A and B are interchangeable.

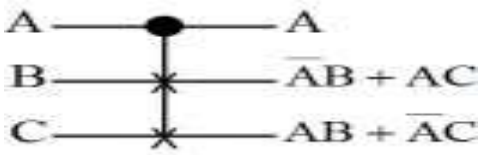

Fig.3.5. Symbol of CSWAP Gate

4. DESIGN OF MULTIPLEXERS, DEMULTIPLXERS, DECODERS USING QUANTUM LOGIC CIRCUITS:

Quantum logic circuits are the logic circuits that are built by using quantum gates and qubits. Quantum computing is the latest technology which can bring a huge change in day to day appliances. Even when quantum computers do work with accuracy, we cannot measure the output without the help of

a classical register as the computations in quantum computers involve qubits and classical computers use binary digits. So a classical register is required for measuring the output obtained from a quantum computer. Quantum gates play a crucial role in build a quantum circuit. As mentioned in the previous chapter, these gates are divided into three types as unary, binary and ternary gate. One of the important quantum gates used in our work for the design of multiplexers and demultiplexers is CSWAP gate. This gate is called Controlled SWAP, comes under ternary gate and is used for swapping the values. As the CSWAP gate is reversible and universal i.e., any logic circuit can be constructed, itis used for the design of multiplexers, demultiplexers and decoders. From the previous chapter it is observed that the output of CSWAP gate is the output of 2:1 multiplexer. In this chapter, we define 2:1 multiplexer 1:2 demultiplexer and their cascading to realize high end structures i.e., 4:1, 8:1 multiplexer and 1:4, 1:8 demultiplexers.

4.1 MULTIPLEXERS

Multiplexers can be built using a quantum gate called 'CSWAP' and the code can be written based on the truth table, quantum circuit or by cascading. Only high-end multiplexers can be built by cascading the low-end multiplexers. Also we can use python code for programming a quantum circuit.

4.1.1 Design of 2:1 Multiplexer

Quantum circuit of a 2:1 multiplexer requires only one quantum gate i.e. a cswap gate. The number of gates required for a circuit depends on the simplified expression obtained from the truth table. From the below circuit, only one cswap gate is applied.

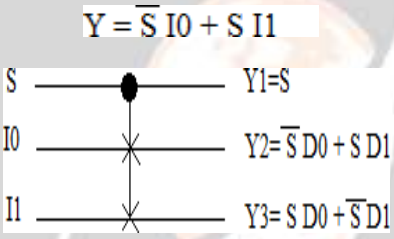

Fig. 4.1: Quantum Circuit of 2:1 MUX

4.1.2 Design of 4:1Multiplexer

Quantum circuit of a 4:1 multiplexer requires three quantum gates i.e. three cswap gates.

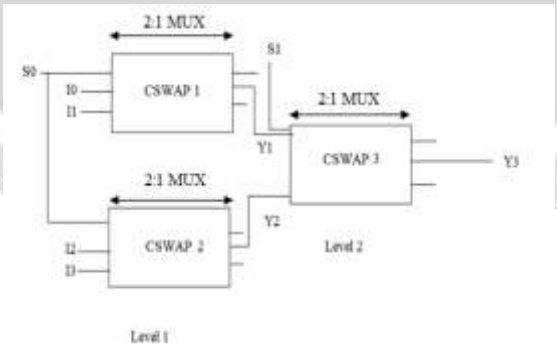

Fig. 4.2: Cascading of CSWAP gates to design 4:1 MUX

4.1.3 Design of 8:1 Multiplexer

Quantum circuit of an8:1 multiplexer requires seven quantum gates i.e. seven cswap gates.

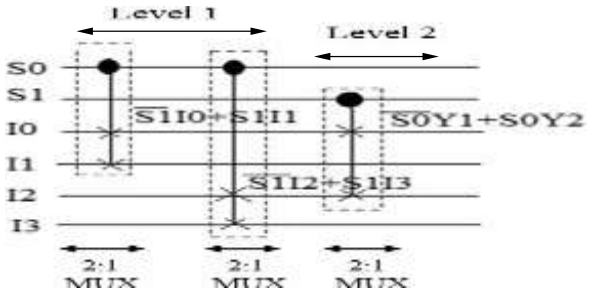

Fig. 4.3: Quantum Circuit of 8:1 MUX using 2:1 MUX

4.2. DEMULTIPLEXERS

Similar to multiplexer, a demultiplexer can be implemented as a quantum circuit. By using 'CSWAP' quantum gate and python code for programming a quantum circuit we can build a demultiplexer. Also, the code can be written based on the truth table, quantum circuit or by cascading the low end demux.

4.2.1 1:2Demultiplexer

Quantum circuit of a 1:2demultiplexer requires only one quantum gate i.e. a cswap gate.

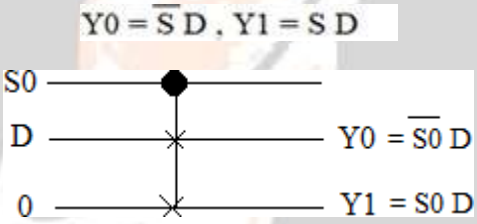

Fig. 4.4: Quantum Circuit of 1:2 DEMUX

4.2.2 1:4 Demultiplexer

Quantum circuit of a 1:4demultiplexer requires three quantum gates i.e. three cswap gates.

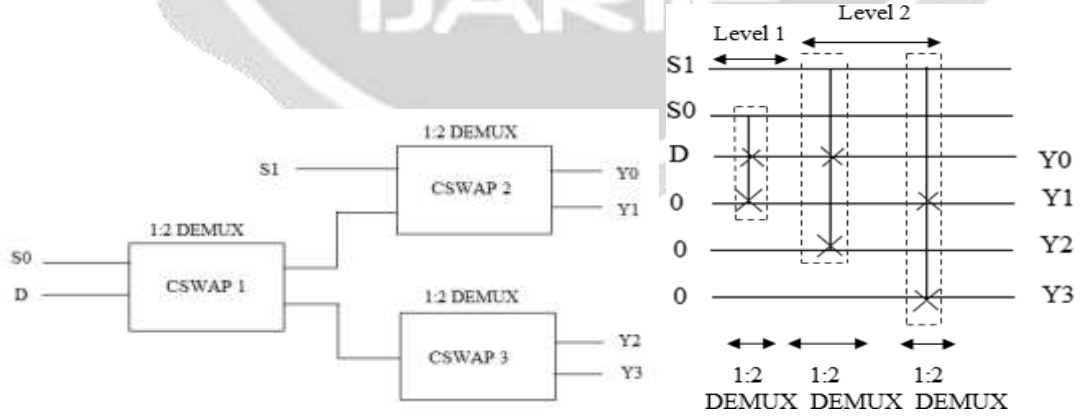

Fig. 4.5: Design of 1:4 DEMUX

4.2.3 1:8 Demultiplexer

Quantum circuit of a 1:8 demultiplexer requires seven quantum gate i.e. seven cswap gates.

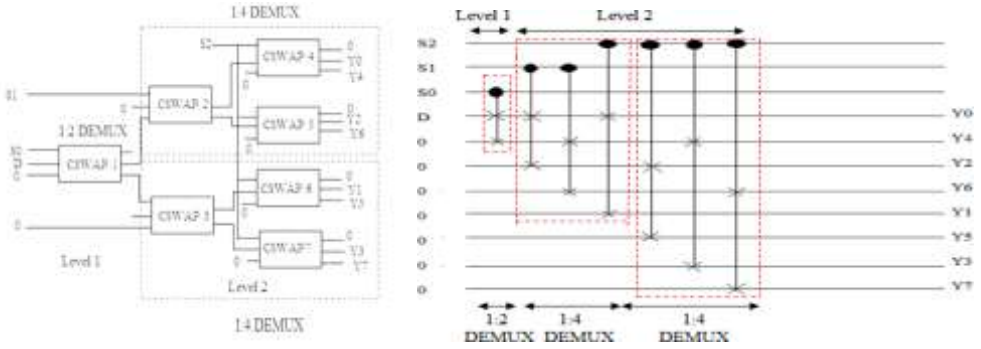

Fig.4.6: Design of 1:8 DEMUX

4.3 DECODERS

Similar to demultiplexer, a decoder can be implemented as a quantum circuit. By using 'CSWAP' quantum gate and python code for programming a quantum circuit we can build a decoder. Also the code can be written based on the truth table, quantum circuit.

4.3.1 2:4 DECODER

Quantum circuit of a 2:4 decoder is same as 1:4 demultiplexer when D=1, which requires three quantum gate i.e. three cswap gates.

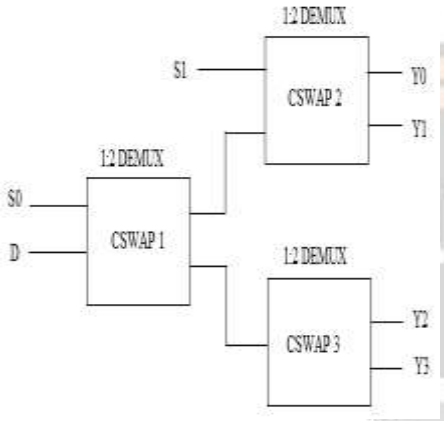

Fig.4.7: Cascading of CSWAP gates to design 2:4 DECODER

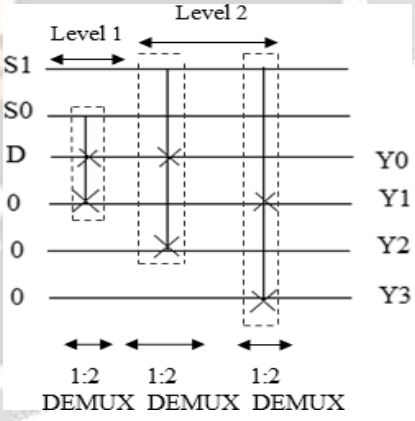

Fig.4.8: Quantum Circuit of 2:4 DECODER

5. SIMULATION RESULTS

Quantum circuits can be built using some open source software's like Anaconda, Jupyter Notebook and IBM Quantum Experience.

5.1 MULTIPLEXERS

5.1.1 2:1 MULTIPLEXER

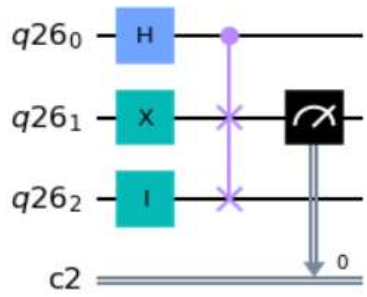

Fig.5.1: Quantum Circuit of 2:1 MUX

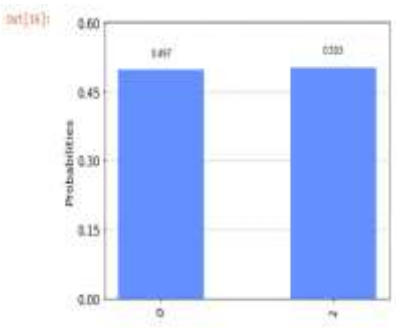

Fig.5.2: Histogram with H gate

5.1.2 4:1 MULTIPLEXER

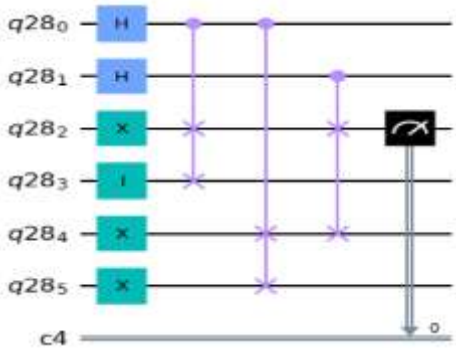

Fig.5.3: Quantum Circuit of 4:1 MUX

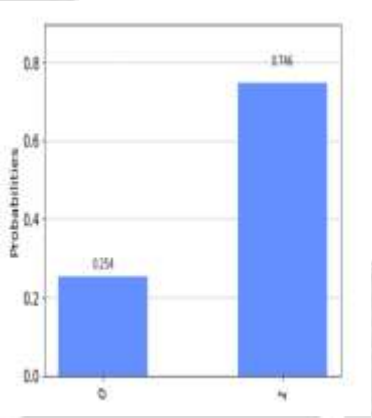

Fig.5.4: Histogram with H gate

5.1.3 8:1 MULTIPLEXER

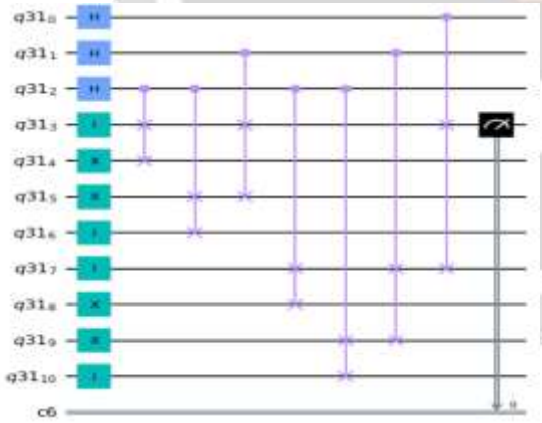

Fig.5.5: Quantum Circuit of 8:1 MUX

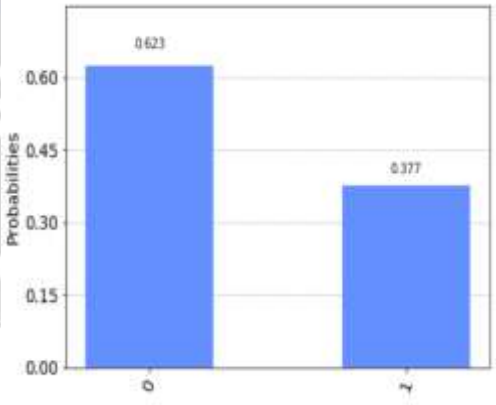

Fig.5.6: Histogram with H gate

5.2. DEMULTIPLEXERS

5.2.1. 1:2 DEMULTIPLEXER

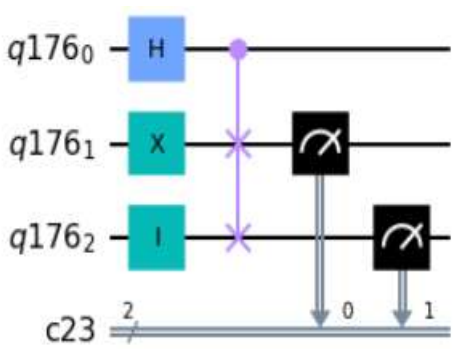

Fig.5.7: Quantum Circuit of 1:2 DEMUX

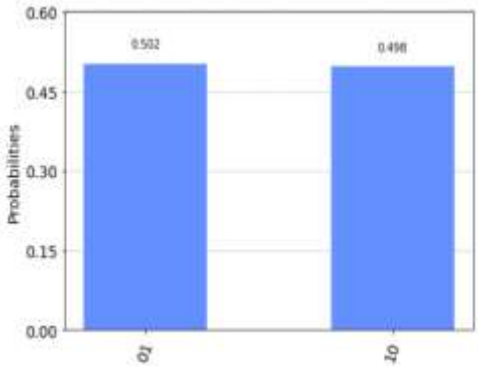

Fig.5.8: Histogram with H gate

5.2.2. 1 :4 DEMULTIPLEXER

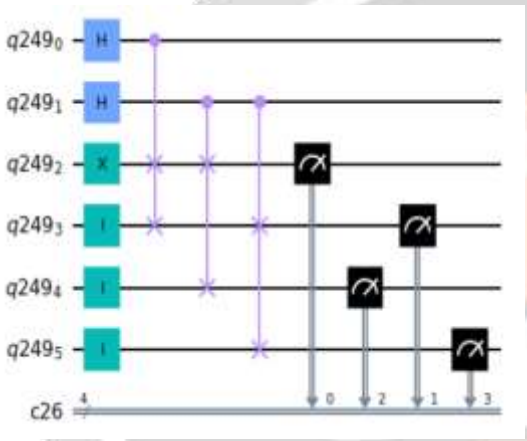

Fig.5.9: Quantum Circuit of 1:4 DEMUX

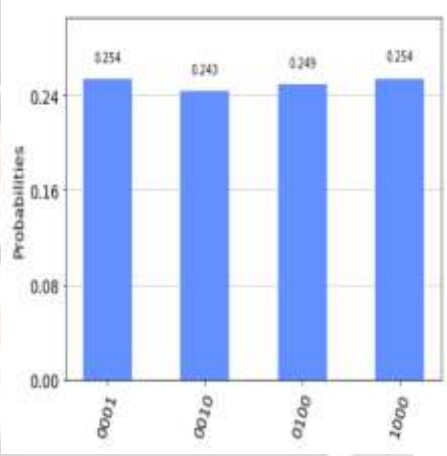

Fig.5.10: Histogram with H gate

5.2.3 1:8 DEMULTIPLEXER

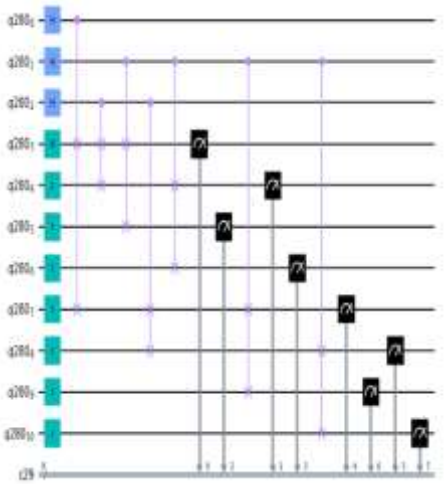

Fig.5.11: Quantum Circuit of 1:8 DEMUX

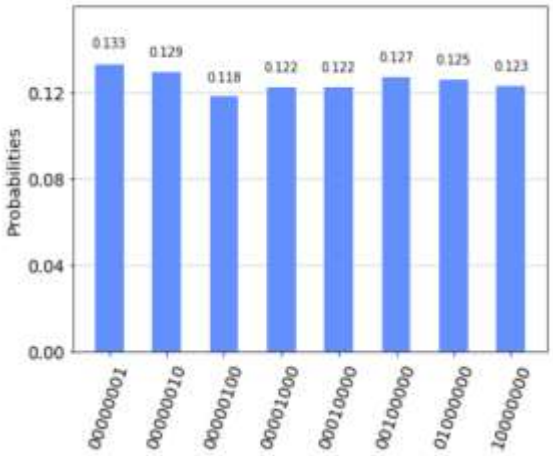

Fig.5.12: Histogram with H gate

5.3. DECODERS

5.3.1. 2:4 DECODER

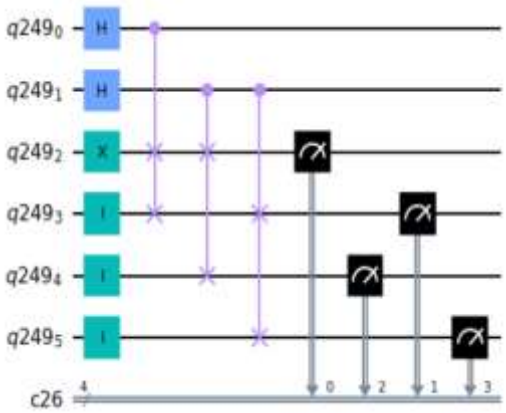

Fig.5.13: Quantum Circuit of 2:4 DECODER

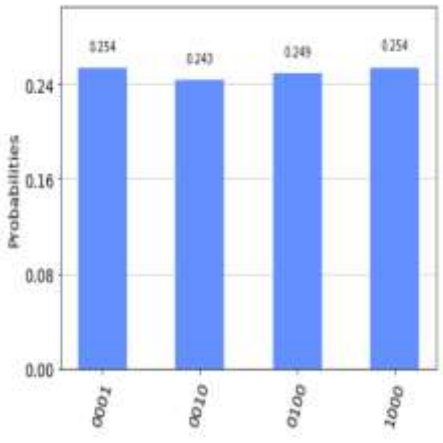

Fig.5.14: Histogram with H gate

6. CONCLUSION AND FUTURE SCOPE

Advancements in the CMOS technology have been in wane to cope up with need of high speed and complex problem-solving requisites that led to develop quantum systems. In this article, the implementation of combinational circuits with quantum gates was presented. Combinational circuits defined using Qiskit were verified with IBM Quantum simulator. Further, a simple method of instantiating these quantum gate-based combinational circuits was proposed to realize high-end logic functions.

In the proposed work, multiplexers and demultiplexers have been implemented using CSWAP gate, and simulated using IBM Qiskit with Python coding. Further, as compared with its implementation using HDL, the classical gates are not required which need large area, high power consumption and low speed.

The low quantum cost multiplexers can be used in the quantum entanglement to decode information at the receiver side with fruitful results. Not only the multiplexer, the demultiplexer can also be used as decoder at the receiver end of the quantum entangler.

7. REFERENCES

[1] W.D. Pan, and M. Nalasani, "Reversible logic," IEEE Potentials, vol. 24, pp. 38-41, March 2005. J.M. Shalf, and R. Leland, "Computing beyond Moore's law," Computer, vol. 48, pp. 14-23, December2015.

[2] T.M. Conte, E. Track, and E. DeBenedictis, "Rebooting computing: New strategies for technology scaling," Computer, vol. 48, pp. 10-13, December2015.

[3] J.D. Hidary, Quantum Computing: An Applied Approach, Springer Nature, Switzerland AG, 2019, pp.3-10.

[4] M. Soeken, H. Thomas, and R. Martin, "Programming quantum computers using design automation," proceedings of Design, Automation and Test in Europe, March2018.

[5] M.S. Islam and M. Rafiqul Islam, "Minimization of reversible adder circuits," Asian Journal of Information Technology, vol. 4, pp. 1146-1151,2005.

[6] C. Degen, F. Reinhard, and P. Cappellaro, "Quantum sensing: Reviews of modern physics," vol. 89, pp. 035002, July2017.

[7] M. Krenn, M. Malik, T. Scheidl, R. Ursin, and A. Zeilinger, "Quantum communication with photons," Optics in Our Time, Springer, December2016.

[8] A. Anand, B.K. Behera, and P.K. Panigrahi, "Solving diner's dilemma game, circuit implementation and verification on the IBM quantum simulator," Quantum Inf. Process. vol. 19, pp. 1-14, May2020.

[9] V. Vedral, A. Barenco, and A. Ekert, "Quantum networks for elementary arithmetic operations," *Physical Review A*, vol. 54, no. 1, pp. 147–153, July1996.

[10] S. A. Cuccaro, T. G. Draper, S. A. Kutin, and D. P. Moulton, "A new quantum ripple- carry addition circuit," *CoRR*, vol. abs/quantph/0410184, November2004.

[11] H. Thapliyal, "Mapping of subtractor and adder-subtractor circuits on reversible quantum gates," Trans. on Comput. Sci. XXVII, LNCS 9570, pp. 10–34, April2016.

[12] M. Rahmati, M. Houshmand, and M.H. Kaffashian, "Novel designs of a carry/borrow look-ahead adder/subtractor using reversible gates," J. Comput. Electron., vol.16, pp. 856-866, July2017.

[13] G. Oktay, K.T. Weng, B-F. Kent, and A. Brodutch, "Benchmarking quantum processors with a single qubit," Quantum Inf. Process. vol. 19, pp. 1-17, March2020.

[14] J. Wang, and K. Choi, "A carry Look-ahead adder designed by reversible logic", Proceedings of IEEE International SoC Design Conference, pp.216-217, November2014.

[15] M Perkowski and P Kerntopf, "Reversible logic", Proceedings of International Conference on European Microwave Association, pp. 1-12,2001.

[16] J.W. Bruce, M.A. Thornton, L. Shivakumaraiah, P.S. Kokate and X. Li, "Efficient Adder Circuits based on a Conservative Reversible Logic Gate", *Proceedings of IEEE Computer Society Annual Symposium on VLSI. New Paradigms for VLSI Systems Design*, pp. 83-88, April2002.

[17] T.S. Humble, H. Thapliyal, M-C. Edgard, F.A. Mohiyaddin, and R.S. Bennink, "Quantum computing circuits and devices," IEEE Design and Test, vol. 36, pp. 69-94, April2019.

[18] https://qiskit.org/

[19] Weinfurter H eta., "Quantum communication and entanglement," *Proceedings of 2000 IEEE International Symposium on Circuits and Systems (ISCAS)*, August2002.

[20] Y. Syamala and A.V.N Tilak, "Synthesis of Multiplexer andDemultiplexer Circuits using Reversible Logic," Int. J. of RecentTrendsin Engineering and Technology, Vol. 4, No. 3, Nov2010.

[21] ArijitRoy, DibyenduChatterjee and Subhasis Pal, "Synthesis of Quantum Multiplexer Circuits," IJCSI International Journal of Computer Science Issues, Vol. 9, Issue 1, No 3, January2012.

[22] RakshithSaligram, ShrihariShridharHegde, Shashidhar A Kulkarni, H R Bhagyalakshmi and M K Venkatesha, "Design of Fault Tolerant Reversible Multiplexer based Multi-Boolean Function Generator using Parity Preserving Gates," International Journal of Computer Applications (0975 – 8887), Volume 66– No.19, March2013.

[23] Dipak Kumar K et al., " Generalized Construction of Quantum Multiplexers and De-Multiplexers Using a Proposed Novel Algorithm Based on Universal Fredkin Gate," 2016 Sixth International Symposium on Embedded Computing and System Design (ISED), July2017.

[24] Neha P and Neelam R P, "A power-efficient multiplexer using reversible logic," Indian Journal of Science and Technology, Vol. 9, Issue 30, August2016.

[25] Gowthami P and Satyanarayana R. V. S, "Design of a multiplexer using reversible logic," International Journal of Applied Engineering Research, vol. 12, No. 12, Nov. 2017.