Advancements in Quantum Computing - A Review

***R. Madhusudhana[1], K. C. Navyashree[1], L. Krishnamurthy[1], R. Gopalkrishne Urs[2]**

[1]Center for Nanotechnology, Department of Mechanical Engineering, The National Institute of Engineering (NIE), Manandavadi Road, Mysuru, India
[1*]madhu[at]nie.ac.in
[2]Department of Physics, The National Institute of Engineering (NIE), Manandavadi Road, Mysuru, India
[2]rgk[at]nie.ac.in

Abstract: ***Quantum Computing is the rapidly developing research field. This paper gives an insight to the Quantum Computing and its advancements till date. The quantum technique combines the Quantum Mechanics, Computer Science and Classical Information Theory. Here generally, the information will be identified first. Then this information will propagate to cause the quantum computation effect. It has a fundamental position in the physics [3]. However, the mathematical treatment of information, especially information processing, is quite recent and necessary to get error free information. In the classical computation Moore's law was being applied to process the information. But Moore's law will stop being relevant soon, as we are beginning to utilize another type of calculation which is Quantum Computing. For a very long time at this point, computers have been getting smaller and more remarkably powerful. However, in spite of these advances, there are as yet numerous issues that can't be unraveled by amazing PCs and there is no assurance we will have the option to illuminate them yet it might be solved through the quantum processing [9].***

Keywords: Cryptography, Entanglement, Superposition, Quantum Computing

1. Introduction

Quantum computing is a new computational technique which is going to use the two quantum mechanical properties i.e., Superposition and Entanglement [1][2][6]. Superposition means an ability of the quantum system to exist in more than one state at a time and Entanglement is some quantum sense of two particles being together apart from the distance between them [1][9]. The classical computation technique uses only two states i.e., 0 or 1. But quantum computation uses 0,1 and the superposition of the 0 and 1 states. These are called as Qubits (quantum bits) which are analogous to the classical bits. The computer which uses quantum computation is called as Quantum Computers [2]. Quantum Computers solve particular computational problems like Integer Factorization. It computes and solves the problem faster than the old Computers [2]. The Quantum Computers study undergoes in the field of Quantum Information Science. The pioneers of quantum computing are Paul Benioff and Yuri Manin. Here the computation is done by controlling the qubits with the help of quantum logic gates. these logic gates are similar to the conventional logic gates [10].

The whole technique of Quantum Computation is possible due to the spin of the particle which makes it attractive for the Memory Storage, Cryptography and Magnetic Sensor Applications [8].

2. Quantum Computing

It consists of few models to compute the bits, which are the Quantum circuit model, Quantum Turing machine, Adiabatic quantum PC, Single direction quantum PC and Different quantum cellular automata. We can implement a quantum computer using 2 ways Analog and Digital. Simple methodologies are additionally partitioned into quantum annealing, adiabatic quantum computation and quantum simulation. Digital Quantum Computers use logic gates to do calculation. The two methodologies i.e., analog and digital use quantum bits or qubits.

If a classical computer can solve any problem, then it can also be solved by the Quantum Computer. In the same way as given by Church Turing Thesis, if any calculation can be done by Quantum Computer then it is also possible from the classical computer. This means that Quantum Computers doesn't give any extra calculations but provides a force with respect to the time intricacy in certain issues. It also takes care of special issues which is not available in any of the classical computers with respect to time. The investigation of the computational complexity of issues concerning Quantum Computers is known as Quantum Complexity Theory [10].

3. Quantum Operations

It is seen that quantum computers follow Church Turing Thesis [10][1][3]. To carry out quantum calculations, we should these basic conditions: Two-level system (0 and 1) as a qubit, Capacity to prepare the qubit in the given state say 0, Capability of measuring each qubit, Construction of basic gate operations such as Conditional logic gate and sufficient long decoherence time [4].

Superposition of states of the quantum computer will be destroyed if it is not well isolated from the environment [4].

The model of quantum calculation depicts the calculation as far as an organization of quantum logic gates. Consider a memory having n pieces of data and 2n states. These states are calculated by a probability vector. This vector gives the memory which would be in a specific state [3][9][10]. In the classical computational techniques one entry used to be considered as one and all others as zero. But in quantum computers they are generalized to density operators which are also a numerical establishment for the quantum logic gates [3][9][10]. Let us consider a single memory. This memory can hold only one bit which can have 2 states i.e., the zero state or the one state. This is represented using the Dirac notationas follows,

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

A quantum memory then having super position $|\Psi\rangle$ of these classical states 0 and 1 is,

$$|\Psi\rangle = \alpha|0\rangle + \beta|1\rangle = \begin{pmatrix} \alpha \\ \beta \end{pmatrix}$$

here,

$$\alpha 2 + \beta 2 = 1 \qquad (1)$$

Here, the coefficients α and β are the complex numbers and also quantum amplitudes. Ψ is a probability vector. In this situation one bit of information is encoded in the computer memory. This can be determined through computational basis measurement. If you determine a zero state in the memory, then this is due to the probability of α^2. If you determine a one state in the memory. then this is due to the probability of β^2. This condition of one-qubit quantum memory is controlled by applying quantum logic gates, which is similar to old style memory that can be controlled with traditional rationale entryways.

As of now we are working on single qubit. But we can apply the same method to work on multiple qubits. This can be done in 2 methods. In first method we can choose a qubit and apply this entryway to the another qubit which is called as objective qubit. The remaining memory is set free. Another method is to apply the entryway to the objective qubit. This is done when the other part of the memory is in ideal state. By doing this we can get more memory stockpiling, additionally the computational limit is expanded [9][10].

4. Quantum Cryptography

Cryptography holds a notable position in today's electronics. The message, passwords and money exchange also requires the similar kind of security for their work. This privacy and integrity [8]. In these days we use public key cryptographic system almost in every applications and protocols as it has the basic cryptographic algorithm. It uses Number factorization to provide security. This number factorization is not feasible for the large numbers in old computers. But this can be solved by a Quantum Computer as it uses Shor's algorithm and Gover's algorithm. Shor's algorithm is used for Asymmetric cryptography which is based on large prime integer number factorization and discrete logarithm problem. This has so much capacity that it could break several modern asymmetric algorithms. Gover's algorithm is used for Symmetric cryptography to find the factors. this calculates and uses Quantum Computers to look through unsorted information bases. The calculation can locate a particular section in an unsorted information base of N passages in square base of N look. By utilizing these two in number calculations, investigates have been led to make a completely operational inclusive Quantum Computer in future. These capacities in Quantum Computers can breakdown the recent public key cryptographic calculations such as RSA and Elliptic Curve Cryptosystems [7][8].

5. Conclusion

Quantum computing has gained a tremendous interest by the scientists because of qubits. Having the certain number of Qubits, it is possible to run quantum calculations and it has the ability to outflank the present innovation in some particular cases. It can also come up with another alternative for the semiconductor systems. Even though the applications of the quantum computing technique are limited, soon it will be evolved by the implementation of the different algorithms. It will also give a conclusion to the Moore's law. Despite of all these things quantum computers are hard to build since it is more sensitive when it is prone to the environment. Therefore, we should develop more sophisticated environment for it to work which is difficult to build. But it can solve problems which couldn't be solved by even the supercomputers. Soon after some year's quantum computers will take charge and replace the old computers.

References

[1] Gamble S., "What it is, Why we want it, and How we're trying to get it", National Academic Press (US), ISBN 978-0-309-48750-4, 2019.

[2] Metcalfe G., Chow J., "Quantum computers: Are we there yet?", National Academic Press(US), 2018.

[3] Andrew Steane, "Quantum computing", IOP Publishing Ltd, no. 61, 1997.

[4] Shu-Shen Li, Gui-Lu Long, Peng-Shan Bai, Song-Lin Feng and Hou-Zhi Zheng, "Quantum Computing", PNAS, no. 21, 2001.

[5] P. Walther, K. J. Resch, T. Rudolph, E.S Schenck1, H. Weinfurter, V. Vedral, M. Aspelmeyer & A. Zeilinger, "Experimental one –way quantum computing", Nature, 2005.

[6] B. P. Lanyon, M. Barbieri, M.P. Almeida and A.G. White, "Experimental quantum computing without entanglement", The American Physical Society, PRL 101, 2008, 200501-4.

[7] Jay M. Gambetta1, Jerry M. Chow1 and Matthias Steffen, "Building logical qubits in a superconducting quantum computing system", JM Gambetta et al, 2017.

[8] Vasileios Mavroeidis, Kamer Vishi, Mateusz D. Zych and Audun Jøsang, "The Impact of Quantum Computing on Present Cryptography", (IJACSA)

International Journal of Advanced Computer Science and Applications, No. 3, 2018.

[9] Michael Agbaje, “A review of quantum computing and its architecture”, Caribbean Journal of Science, ISSUE 1 (JAN - APR), 2019.

[10] Grumbling, Emily; Horowitz, Mark (eds.), “Quantum Computing :Progress and Prospects”, National Academies Press., ISBN 978 301/479691, 2018