Processing Power of Quantum Computer

Muhammad Zeeshan, Saadia Anayat, Rabia and Nabila Rehman

Abstract— the history of computer start from analytical engine and now a day it is converted into a very fast, more powerful and smaller computer. These traditional computers are based on small IC, logic gats and microprocessors. Development in every field of life like Education, Business and Ecommerce Due to Traditional computers, although traditional computers were more powerful, faster and power saver but their growth has stopped. Now scientists are working to develop a new kind of computers that based on Quantum physics rules which will be totally different from traditional computer. The Quantum computes are more powerful than traditional computers. The Quantum computer will solve those problems which are not solvable by traditional computers. It takes a very short time to compute a transection which traditional computer takes many years to compute. The era of research, development and progress totally changed due to this grate invention. It is accepted that in upcoming years these Quantum computer will take place of traditional computers.

Index Terms— Quantum Computer, Qubit, Traditional computer, Computation

1 Introduction

20th Century has brought many inventions and science has brought a lot of progress such as in the field of computer world. From analytical engine to global world this journey has completed after many inventions. First of all with the using of vacuum tube some computers have made they work properly and do their tasks successfully but the failure of this computer is the inventions of IC chip and logic gats. The inventions of new smart computer that uses Microprocessors are too much fast powerful cheap and in size they are very small. They influence of every field of life such is business, education and personal life etc. every field of live got many progress using these faster computers. But 21th century the theory of quantum computer dissection started this computer which works according to the quantum Physic rule. Quantum computer theory has changed the entire past computer theory and rule of todays. The tasks which is not possible for normal computer it can be solved through quantum computer efficiently. The normal computer takes many years to solve a problem that is solved by quantum computer in too much short time. Normal computer can make one transection at a time but quantum computer will make unlimited transection at a time. The computational processing power is more thousand in time than normal computer. Normal computer has two state 1 or 0. But quantum computer have three states 1 or 0 or any point between 1 and 0. It calls quantum bit or Qubit. The smallest unit of quantum computer is Qubit. The essential building block of Quantum compute is showing with diagram.

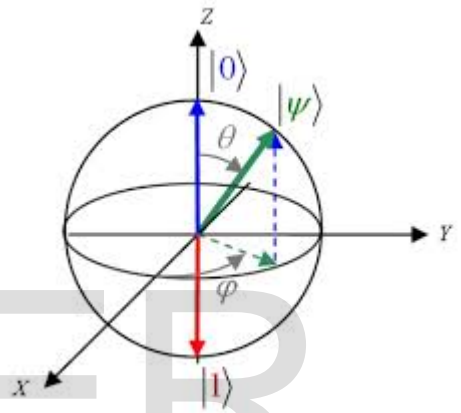

Fig 1: Bloch sphere of Qubit [3]

The Fig 1 is the pictorial view of Qubit. Qubit is the basic building block of Quantum computers. Which are totally different from bits. A single bit can store a value of 0 or 1 bit Qubit can store a lots of information any point between 0 and 1.

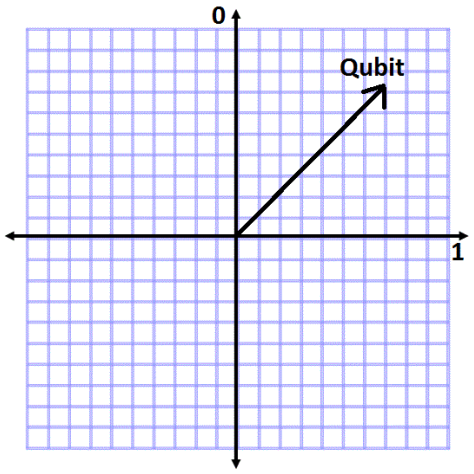

Fig 2: Qubit

- ***Muhammad Zeeshan*** *is with Department of Computer Science & Information Technology as a student of MSCS at VU, Lahore, Pakistan. He is currently an employ of FCSC Peshawar, under Ministry of Defence Islamabad,Pakistan E-mail:ms150400558@vu.edu.pk*
- ***Saadia Anayat*** *is with Department of Computer Science & Information Technology as a student of MSCS at VU, Lahore, Pakistan. E-mail:ms150401012@vu.edu.pk*
- ***Rabia*** *is with Department of Computer Science & Information Technology as a student of MSCS at VU, Lahore, Pakistan. E-mail:ms150400912@vu.edu.pk*
- ***Nabila Rehman*** *is with Department of Computer Science & Information Technology as a student of MSCS at VU, Lahore, Pakistan. She is currently working as a Computer Science Teacher in Punjab School Education Department Dist. Khanewal E-mail:ms140400059@vu.edu.pk*

Figure 2 shows the Qubit a point between bit 0 and 1. With the invention of quantum computer changing is accepted in every field of life especially physics, mathematic, engineering and chemistry. The rules of these subjects can be changed totally. Scientist says that the quantum computer will abolish all the ICs and security code of normal compute. The probable processing power of quantum computer actually confuse the mind because a quantum computer basically function as a huge similar processing machine, it can work on millions of calculation simultaneously while a traditional computer works on one calculation at a time, in sequence. In quantum computers with thousand Qubit, the D-Wave 2X system can examine through 2^{1000} probable explanations simultaneously.

Quantum computing is an emerging filed which uses new types of hardware and method of computation based on quantum mechanics. Quantum computing make exclusive new algorithm taking advantage of quantum behavior, to get significantly faster computation, this makes large scale more complex problem also become addressable. Quantum algorithm is implemented by quantum circuits which are comprised of quantum gates which act upon quantum bits or Qubit. Using superposition one can simultaneously represent all possible input combination so with N inputs one can process 2^N combination in parallel.

At quantum level, constructive interference used to increased probability of correct result. Destructive interference to lessen probability of incorrect result upon measurement.

TABLE 1. COMPARISON OF QUANTUM AND TRADITIONAL COMPUTER

Here we present a table of comparison between quantum and traditional computers.

Comparison			
No	Description	Traditional	Quantum
1	Storage mode	0 or 1	Qubit(any point between 0 and 1)
2	Processing logic	Expending bit and logic gates	Expending conditions of atoms
3	Transport of Information	Information can be copied without spreading	Information cannot be copied without spreading
4	Security	Cannot secure by Hacker attack	Much Secure due to high security alarm
5	Noise acceptance	Noisy channel can be used for communication	Required noise less channel for successful communication
6	Performance of information	Unidirectional	Multidirectional
7	Capacity of computation	One at a time	Multiple at a time
8	Processors	One or more	Approximately 10^{150}

2 RELATED WORK

The Quantum handling component is a computational component that practices quantum computer ideologies to execute tasks. QPU was founded on quantum mechanics. QPU holds computational states in the kind of quantum automatic state. Qubit is the most commonly used instances that refers a stat inside a two dimensional Hilbert space that states were holds in quantum physical organization. For the persistence of precision we define a quantum register as an addressable array of two level quantum physical organizations. We will mention the individual system inside the register as a quantum register component and postulate that each register component can holds Qubit of information. Processes on the quantum register are released by gates like traditional computers quantum gates resemble with well-defined transformation of the computational conditions. Quantum computational prototypes clear in what manner the register and gates inside QPU released quantum computation. Although all the prototypes offer identical computational power from a difficulty viewpoint they change with deference to hardware implementation and ideology of process.

The procedures case for a QPU began by making the quantum register in well present preliminary states and then applying an order of gates that may act on separate or numerous register components. This is commonly mentioned the QRAM model.

The computers computational powers is based on number of transistor that are used and according to Moore's law computers processing power doubles after every two years. As the record of 2014 the high processing power processor 18 core Xeon Has well with 45 MB cache has over than 5.5 billion transistors. With compare to it IBM storage controller is more modern that has 7.1 transistors with 480 MB L4 cache. These much powerful processors are the part of server machines. Other hand still high performance computing demands more powerful processors than currently available processors. Quantum computing is an interiorly a new kind of way to build computer using quantum machines. Quantum machines are very small physics. The laws of physic that is put on microscopes are entirely different then classical physics. Put on laws of quantum machines on to computation will speed up the processing power over classical computers. Quantum computer is a new tool for computer scientist to develop and increase the computation power capacity more batter then use of classical computer.

Within few years every filed of life become a part of computer science. Due to a large number of computers network many of company are try to develop their business fully dependent of web based data application. Due to vast use of internet and social media, email the data on web is increase in a large number of size. The issue of big data analyses is become complicated day by day. There are still many problem that are not solved in polynomial time by traditional computer here the need of something new like quantum computers based on physics quantum rolls. Quantum computer have capability to processing 2^n for n Qubit input. The promos of quantum computer are that traditional computer can solve one problem in years it solve it in few second.

2.1 Quantum Mechanics:

Quantum mechanics is concerned with the behavior of the particles at the quantum level, which differ from that of matter at the macroscopic level. Two key characteristics are:

2.2 Superposition:

A quantum particle can be in multiple states at the same time until measured. Examples include photons (polarization), Elections (Spin), etc.

2.3 Entanglement:

Quantum particles can be joined together in precise way that a measurement of one will determine the probable quantum states of the others.

3 HISTORY OF QUANTUM COMPTER

Shor's algorithm solves many problems in polynomial time like discreet logarithm and integer factorization problem, quantum Factorization. In 1994 Shor's algorithm was expressed. Shor's algorithm takes polynomial time to factor out N integer on quantum computer. The Wiesner's protocol was the quantum cryptographic protocol that is used for quantum money, and BB84 protocol is also used for key exchange. For quantum money Wiesner's protocol stimulated BB84. These both protocols depend on quantum no cloning theorem. Shor's algorithm will be used to spread out public-key cryptography, the first convincing truly example was Diffie and Hellmen's key exchange protocol. These leases two parties agree on a secret key lacking any previous secret knowledge. This key can be used for a symmetric cryptosystem, or as a one to one pad. Although Shor's algorithm present that factoring is well-organized.
On 2007 D-Wave the world largest company of Quantum computer successfully build 1st quantum computer. That 16-Qubit quantum computer solved many problems like pattern matching and image processing.

On May 11, 2011 D-Wave Company published that they build 128Qubit processor "Rainier". That processor is based on adiabatic quantum algorithm. It is much faster processor than old 16 Qubit Processor. The D-Wave one was the first computer that uses 128 Qubit Processor. D-Wave Company clime it was the world 1st computer system that is available for commercially. It is too expansive Quantum computer system approximately price is US$10000000. That system can solve problem of discrete optimization [4].

On 2015 D-Wave launched the world 2nd commercially available Quantum computer. The CPU that used in it was 512Qubit. These computers are designed using Quantum annealing to solve the complex problem as Quadratic annealing binary optimization. The D-Wave 2x Processor has capacity to evaluating 2^{1000} possible solution at the same time.

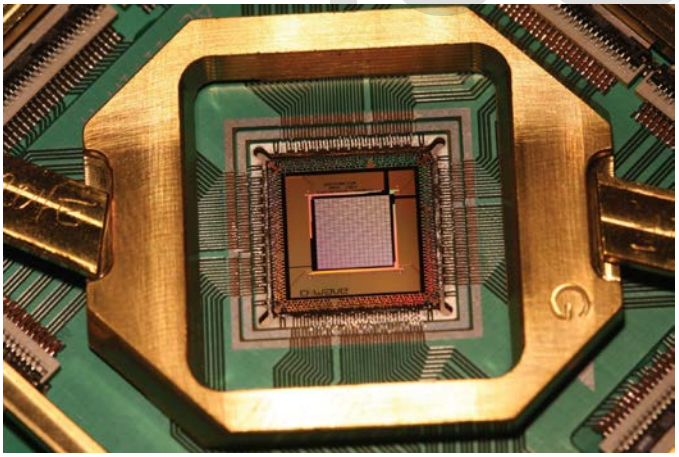

Fig 3: D-Wave 2x Processor [5]

4 TYPES OF QUANTUM COMPUTER

4.1 Silicon Quantum computer

Is a kind of computer that builds using electron spin as a smallest unit. These types of Quantum computers are consist on electron spin and algorithm that simulate the movement of Electrons. The hardware implementation of Silicon Quantum computers are now under construction.

Fig 4: Silicon Quantum Computer

4.2 Optical Quantum Computer

The smallest unit of Optical Quantum computers is photon of light. Optical Quantum computers change their states according to polarization of light. Like traditional computers has 0 and 1, Qubit of optical computers represent |x> Horizontal polarization and |y> the Vertical polarization.

Fig 5: Optical Quantum Computer

4.3 Gate model quantum computing

Logic gates/ Digital gates are the basic building blocks of traditional computer. But in the quantum computer, quantum is used which is equivalent to those digital gates and provides more efficient results. Largest gate model quantum computation takes very less time to compute something which traditional computer takes years to compute it.

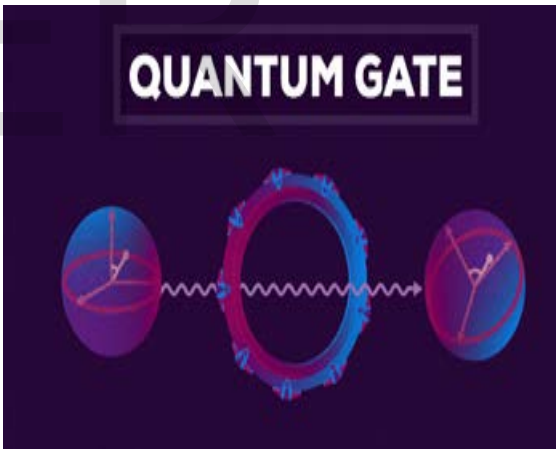

Figure 6: Gate model quantum computing

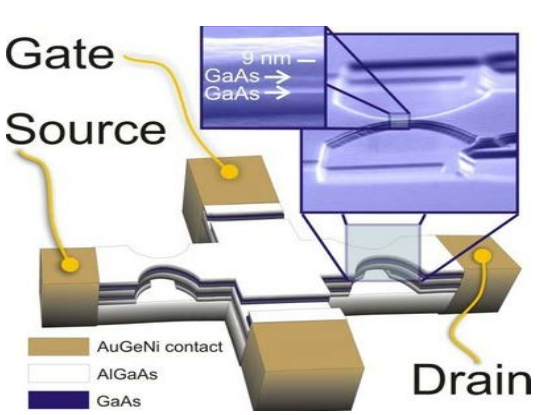

Figure 7: Quantum gate transistors

4.4 Ion trap quantum computing

As a Qubit, Ions are used in this type Of Quantum computing. A scientist named Paul has done successful work on Ion trap quantum computing. Due to his great work, he got Nobel Prize physics. Using electromagnetic field charged atomic particles are imprisoned and postpone in free space.

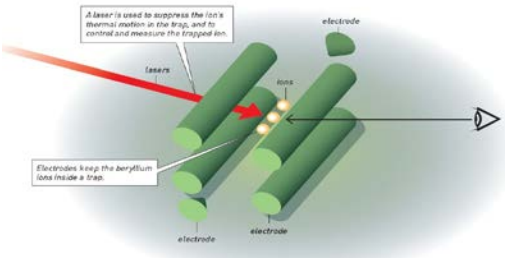

Figure 8: Ion trap quantum computer

4.5 Secure Quantum computer

Quantum computer promises secure communication, developing a quantum computer and secure communication network is a global race. The key advantage of quantum computer is to make secure communication and transfer information between quantum computer networks.

4.6 D-Wave Quantum Computer:

In the year 2007 D-Wave Company lunched first Quantum computer that use 16 Qubit to solve many problem like pattern matching.

4.7 D-Wave one

In 2011, D-Wave company successfully build and run D-Wave one, with 128 Qubit processor named "Rainier". That system can solve problem of discreet optimization. It is too expansive Quantum computer system approximately price is US$10000000.

Fig 9: D-Wave one

4.8 D-Wave 2x

With the sponsor of Google, NASA, Lockheed Martin and University of Southern California D-Wave lunched a new kind of computer much powerful. With 1000 Qubits, the D-Wave 2x system can search through 2^{1000} possible solutions simultaneously. This system is based on Quantum annealing algorithm and it has processor with 512 Qubit.

5 Quantum Languages

The Quantum programing language has capability to deal with the movement of partials like entanglement. Because quantum computation machine are based on quantum physics roles. [7] QCL (Quantum Computation Language) tries to minimize the issues that become barrier to adoption of Quantum computer. It tries to solve issue like Dirac notation, matrices, gates, operators, etc. QCL is architecture independent and high level programing language for Quantum computers. It has capability to implement Quantum algorithm. [8] Quantum computer has physically and logically different from traditional computer the language that used for configuration of a traditional computer was not be able to configuration a Quantum computer in [9] tries to evolves high level circuit gats, language. Quipper is the language that is surrounded and scalable programing language for quantum computers. It elaborates quantum libraries like quantum integer and fixed point arithmetic. It involves gate by gate execution of circuit, much powerful to manipulation of circuits. In [10] show the extension of C++ for Quantum computers. It used to implementation of basic Qop function like QFourier, QSwap, QNot, QHadamard. New area of research for Quantum programming language are still need many evaluation, existing language of traditional computers are enough, cannot compatible for Quantum computer.

6 High Performance Quantum Computing

Many problems which need much computation power to solve that are not be able to solve by traditional computer can be solved by Quantum computer. High performance quantum computer will simulate many hard problems and result in $1x10^{15}$ floating point number per second [11].
Quantum information processing for multiple user high performance quantum computers have a huge 3-dimensional cluster is operated generic resource.

Quantum computing application areas include:

1. Image processing
2. Drug discovery
3. Cyber security
4. Finance
5. Logistics
6. Weather modeling
7. Genetics analysis
8. Signal processing
9. Physics modeling
10. Chemical reaction modeling

7 Quantum Entanglement

In Quantum entanglement, numerous elements are linked organized in such a way that the capacity of one element's quantum state controls the probable quantum states of the further components.

A quantum mechanical miracle in which the quantum states of two or more substances have to be defined with orientation to each other, yet the discrete substances may be spatially disconnected.

The interval is a nascent possession in the forthcoming into presence photon by the photon with the impulsive captivation an

emanation of light compared to the particles and the waves of light that previously occur. The wave element dualism of light is establishing a collaborative development with the forthcoming into presence compared to the waves of light on the vitality and impetus of our own movements. Consequently, we have quantum entanglement among waves comparative to new photon alternations inside a development of incessant energy altercation or incessant formation.

Quantum entanglement means that if two objects are quantum mechanically entangled, then these two objects are related to each other even there is a huge distance between them. It means there is a superposition of bits (0, 1) or all at the same time.

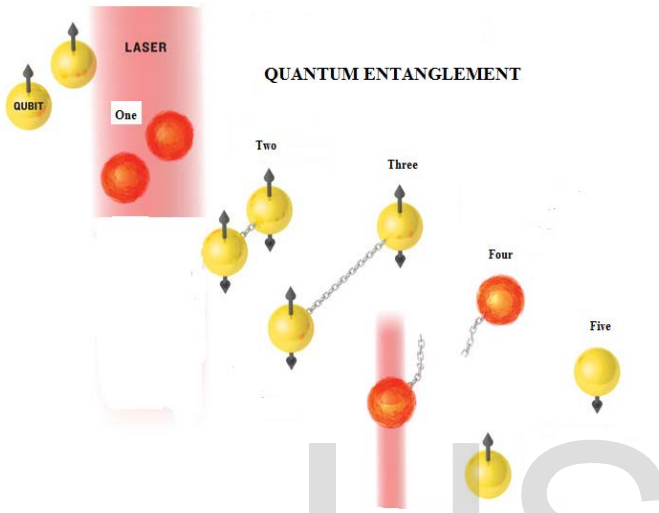

Figure 10: Quantum Entanglement

In this figure unlike ordinary bit of information, Qubits can be linked in a way that has no analog in the digital world. This linkage, called entanglement, acts instantaneously over any distance.

In the first stage, two qubits are entangled through the action of a laser. In the second stage, once they have been entangled, they are in an indeterminate state. In the third stage, the qubit then can be separated by any distance, but they will remain linked. In the fourth stage, when one of the qubits is manipulated __ say, to perform a step in a quantum computer program__ the manipulation happen instantly to its entangled twin as well. In the fifth stage, if the manipulation includes reading the state of one of the qubit, the entanglement ends, and both Quits states are revealed.

8 Computational Power Of Quantum Computers

First time on 1981 Richard Feyman presents the theory of quantum that based of physics principles and many companies start making hardware of quantum computer. But argue start between scientists that what quantum computer can do? And what cannot. People of computer science can ask the question can quantum computers solve the problem which classical computer cannot solves? Like problem of NP class or NP complete class. The answer is NO quantum computer cannot solve problem of NP class, because algorithm can be exists to solving these problem.
Quantum computer promise to give result of a problem in seconds that traditional computer can take many years to solve. For N number Quantum Computer compute 2^N observation simultaneously it's very hard problem for traditional computer. Quantum computer can very easily read secret messages that travel on the internet, transfer by a traditional computers. Quantum computers are very useful to playing with big Data, a needle in a haystack. For example finding two equal numbers from a 10 million numbers, Quantum computers can do in short time but traditional computers perform 10 million steps.

8.1 Quantum Algorithm

The Quantum algorithm designed to evolve the quantum state of a system so that when a measurement is taken, the probability of the correct result is increased and the probability of incorrect result is decreased. Some algorithm gives a result with certainty and other give result with probability. Quantum algorithm is in areas of active research-areas including factoring searching, solving system of linear equations. Deutsch algorithm first to show a definite advantage of quantum computing over traditional computing. There is a collection of quantum Zoo on NIST (national institute of standard and technology).

Quantum computing associates with the base of mathematics and physics. Grover's algorithmic technique is used to increase the processing power of quantum computers over traditional computer.

For searching purposes on a quantum computer, Grover's algorithm performing very nice and speedup than traditional computers. The classical algorithm requires O (N) time for searching in other data, but Grover's algorithm needs only $O(\sqrt{N})$ operations.

Peter Shor's algorithm is a very famous algorithm in publications of quantum computer. It solves factorization of integers in polynomial time.

The Simon's problems can speedup exponential time over traditional computers in querying from Black-box. Best algorithm probabilistic need exponential queries to the black box functions in order to define a Simon's quantum algorithm used polynomial time to solve these problem execution only optimal (n) queries.

8.2 Quantum Cryptography

Cryptography is the study of data security for the resolution of the protected communication and broadcast of data. Quantum cryptography is defined as a set of quantum powered possessions used to achieve cryptographic system. The generally well-known illustration of quantum cryptography exists the quantum Key distribution. The cryptographic measurements as well as the approaches are extra protected using quantum cryptography by way of the repetitive structure requirements unique interval significant interchange for a secure material interchange which an achievement by the quantum communication station.

The quantum key distribution schemes used for significant interchange and the process is distributed in two phases and the communication between the two locations is changed a quantum and communal station correspondingly. The protocol identifies interfering if someone tried to hack with extraordinary accuracy.

The quantum superposition rule has permitted new aptitudes which are more extreme than the conventional procedures for information removal and distribution.

The quantum organizations are willing to indiscretion. Caused by trepidations from the surroundings qubits can convert tainted which will consequence in the loss of info. The present procedures used in quantum communication deficiencies the devices which can redevelop the signals. Redevelopment will decrease the chance of ruined data. If appropriate strategies will

not use, then the original signal can be ruined or totally reformed, if by some means more or less techniques established to increase the indication then the similar technique can be used for hacking the signal.

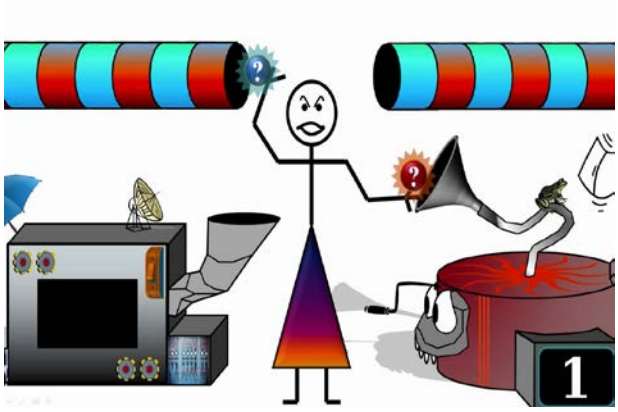

Fig 11: BB84 Quantum Key distribution

8.3 Security & Quantum computing

Conventional computation and security expertise are a practical elucidation for the existing situations, however, in imminent when quantum computers will be operative then lots of changes will be compulsory regarding security and communications. In notions regarding message assault cognate to signatures and encryption cognate cipher text assault are defined and then these are utilized for the initials & encryption organizations construction. For initial, it is demonstrated that they can be erected from slightly needs a purpose which is impact impervious and for encryption. It is demonstrated that they can be erected from public key & symmetric key. Oppositions in quantum computation are withal manageable as they are in the conventional computation, on the other hand, the conventional computation will turn into anxious if communicated with quantum opponents. The leading aims are the reason that Quantum cryptography is considerable extra protected than the conventional computation. Initially, the unfamiliar quantum state cannot be emulated consequently no can capitalize on the unfamiliar state, furthermore some endeavor to calculate and quantify the quantum state determination create a perturbance in the method, consequently and communication which is diverted by some observer determination become infested and drive to be of no avail for the beneficiary. However, if some quantum assets is quantified and transmuted. It cannot be inverted to its pristine state, so these properties potentates the quantum computation, then make it secure from some observer. High caliber research is compulsory in command to systemize the quantum data and cognate protocols, and quantum computing cognate physical layer implementation. The hardware which will be obligatory for quantum computation will be kinder to QKD message schemas. QKD besides quantum message, equally involve receivers & transmitters for impuissant signals or single photon. The best feature of quantum computers in their security. Theoretically verbalizing, it is infeasible to hack the quantum computer method. Quantum computers use observer effect. In this if they endeavor to quantify parameter of a micro particle will be adjust another parameter. This phenomenon, ought to resolve the main issue of classical communications. Each endeavor to spy on a communication will adjust the transmitted message. Observer & alleviating of the quantum pointers can be confined by the quantum closure which makes utilization of the distinctive organization of the quantum pointers, on the other hand for this security quantum transmitter & receivers will be essential.

9 Conclusion and Future wirk

In this paper we try to analyses the new concept, Quantum computing. The implementation issue and challenges of the quantum computing can be discussed in such a way to understand what quantum computer can do and what still cannot solvable by Quantum computers. The area of Quantum computer is still evolving. There may need many thinking to discover new faster algorithm and programming language for Quantum machines. Many problem of real world those are unsolvable by traditional computers will become solvable by Quantum computers. The quantum computers are an excessive viewpoint & it will elucidate lots of issues which cannot be elucidated by conventional Computing. The hardware & software package cognate to Quantum computing are quiet, evolving, however anon it will become an authenticity & will transmute the expertise prospect. The research work is presence completed in quantum languages & quantum algorithms in imperative engender incipient languages for the quantum computers. The work is withal being completed in connection to the security & involution of the quantum computation on demand to get secure & reliable quantum systems. Quantum computers after apprehended will transmute the whole conception of computing, the speed & the computation will increment by lots of times. The hardware, programming language & algorithms will withal alter. The quantifications of security, involution & cryptography will additionally alter. Thus the quantum computers will transmute the whole thing cognate to computers as they ken it. It will engender a lot incipient prospects cognate to jobs & business. It will engender a lot of money & economies will embellishment. Incipient research areas will open the doors for incipient developers. The issues which are appear not decipherable through conventional computing stance an excellent chance to give results utilizing quantum computing. Every single arena of existence, containing research, schooling, engineering, aerospace, medical, expertise, media, nuclear expertise, space peregrinate, armed forces & sports, truthfully, every arena of existence will be pretentious by the quantum computers. Practical quantum computers are withal presence established D-wave, which is accommodating a great purport in different worldwide corporations. General research is withal going on at the University of Waterloo cognate to quantum computation. The inside elevation power quantum computers are quite a vision of the scientist, but some corporations & research organization constructed dominion categorical quantum computers for experiment purport of NASA & Google for immensely colossal knowledge analysis. D-Wave Corporation first presents 512 Qubits quantum computer that is still dominion concrete, however commercially existing on the market. Now D-Wave Corporation starts cerebrating to construct a secure quantum communication network & high performance quantum computing. D-Wave company start thinking to build a secure quantum communication network and high performance quantum computing. After a few years it become possible that general purpose universal quantum computer replace traditional computer. Need for general mean of specifying and controlling quantum computers and their computation.

Acknowledgements

Our special praise to **Hazrat Muhammad (PBUH)** from the deepest core of my heart is forever a model of guidance and knowledge for the whole mankind. The very special entity Allah has brought into our lives, whose saying learns from cradle to grave, awakened the strong desire in us to undertake this course of study write up of this manuscript.
We would like to express our special thanks of gratitude to our course teacher **Dr. Sarmad Abbasi**. Who gave us the golden

opportunity to do this wonderful paper on the topic "**How Data Hazards can be removed effectively**", which also helped us in doing a lot of Research and we came to know about so many new things. His knowledge about research helped us much in planning this paper. His critical suggestions helped shaped and consequently complete this paper. We really thankful to them

References

[1] Noor-ul-Din, Atta-ur-Rehman Muhammad Nadeem, Abdul Ghafoor Abbasi "Quantum Cryptography Trends: A Milestone in information Security" Nov 2015.

[2] Y.Takahashi "Computational power of Quantum circuits with a small number of steps" Dec 2014

[3] https://en.wikipedia.org/wiki/Qubit

[4] "Learning to program the D-Wave One"Retrieved 11 May 2011.

[5] http://www.dwavesys.com/quantum-computing

[6] R. Nicole, "Title of paper with only first word capitalized," J. Name Stand. Abbrev., in press.

[7] Peter Selinger, "A Brief Survey og Quantum Programing Language" Springer 2004.

[8] Bernhard Omer, "The QCL Programing Language".

[9] B.Raja, M. Anand, S. Ravi "Quippeer based implementation of quantum crypto scheme" jan 2015.

[10] https://quantiki.org/wiki/quantum-programming-language

[11] Sergey Edward Lyshevski, High Performance Computing and Quantum Processing, 2012.

[12] Abir U. lgamberdive, Nikita E, Shklovskiy-kordi "Computational Power and generative capacity of genetic systems" Jan 2016.

[13] Joseph F, Fitzsimons, Michal Hajdusek "Post hoc veriication of Quantum computation" Dec 2015.