International Journal of Scientific Engineering and Applied Science (IJSEAS) - Volume-1, Issue-6, September 2015
ISSN: 2395-3470
www.ijseas.com

Understanding Quantum Computing

Dr. K J Sarma, SMIEEE;
Dept of Humanities and Mathematics & Academic cell
Malla Reddy Engineering College (Autonomous), Secunderabad, India,

Abstract: It has been decided that Quantum Computing (Q.C.) should be pursued, as it would be one of the priority research areas of the future having a potential for computational technology development and growth. Hence there is a need to motivate and involve youngsters in research activity related to quantum computing. There is a need to keep the youngsters informed of the what, why, where, when, how of quantum computing. A review of the origin and the progress of the developments in Quantum Computing is made In this paper the author tried to review various aspects of the Quantum Computing like Architecture, Operating system, Infrastructure required if any, links with other computing technologies, Uses, Examples, Theoretical & Practical and class-room Applications, Challenges, Algorithms, Security issues and Future trends.

***Key words**: Quantum computing, Quantum mechanics, qubit, quantum information, quantum mechanics, Richard Feynman.*

1. Introduction

Quantum computing is one of the hottest topics of 21 st century. This is a computational process that uses the quantum mechanical phenomenon different from the usual digital computers. Quantum computing studies theoretical computation systems that make direct use of quantum-mechanical phenomena, such as superposition and entanglement, to perform operations on data.
" It is very interesting and well worth noting, that a quantum system of 500 qubits already requires 2^{500} amplitudes to fully describe its quantum state. This number is larger than the estimated number of atoms in the universe and this enormous potential computational power is well worth harvesting." M.A. Nielsen and I.L. Chuang [26]

The digital computers operate with the help of transistors. Digital computers require data to be encoded into binary digits (bits), each of which is always in one of two definite states (0 or 1), and the memory is made up of the bits. The binary digits for data encoding quantum computation uses **qubits** (quantum bits), which can be in **super-positions** of states.
A Quantum Turing machine [40] is a theoretical model of such a computer, and is also known as the universal quantum computer. Quantum computers share theoretical similarities with non - deterministic and probabilistic computers. In other words a quantum Turing machine (QTM), also a universal quantum computer, is an abstract machine used to model the effect of a quantum computer. It provides a very simple model, which captures all of the power of quantum computation. Any quantum algorithm can be expressed formally as a particular quantum Turing machine. Such Turing machines were first proposed in a 1985 paper written by Oxford University physicist David
Deutsch suggesting quantum gates could function in a similar fashion to traditional digital computing with binary logic gates[41].

Quantum Turing machines are not always used for analyzing quantum computation. The quantum circuit is a more common model. These models are computationally equivalent.
Quantum Turing machines can be related to classical and probabilistic Turing machines in a framework based on transition matrices, shown

by Lance Fortnow [42]. Iriyama et. al have developed a model of a Linear Quantum Turing Machine (LQTM). This is a generalization of a classical QTM that has mixed states and that allows irreversible transition functions. These allow the representation of quantum measurements without classical outcomes [43].
A quantum Turing machine with post selection was defined by Scott Aaronson, who showed that the class of polynomial time on such a machine is equal to the classical complexity class PP [44].

The field of quantum computing was initiated by the work of Yuri Manin in 1980, [2] Richard Feynman in 1982 [22], and David Deutsch [41]. A quantum computer with spins as quantum bits was also formulated for use as a quantum space–time in 1968. Experiments have been carried out in which quantum computational operations were executed on a very small number of qubits. Both practical and theoretical research continues in an effort to develop quantum computers for civilian, business, trade, and national security purposes, such as cryptanalysis.
Large-scale quantum computers will be able to solve certain problems much more quickly than any classical computers that use even the best currently known algorithms, like integer factorization using Shor's algorithm [30] or the simulation of quantum many-body systems. There are quantum algorithms, such as Simon's algorithm, that run faster than any possible probabilistic classical algorithm.[8] When sufficient computational facility is available a classical computer could be made to simulate any quantum algorithm, as quantum computation does not violate the Church–Turing thesis.

2. History & Genesis Of Quantum Computers:

3.

In the following we trace the origin and the genesis of Quantum Computing. There have been great developments in VLSI designs since the introduction of valve technology. In recent times along with the thinking of optimization of performance greater miniaturization of the systems also took a big leap [18**].** It seems the miniaturization has almost reached saturation. Also if transistors are reduced in size further it would hinder the research in quantum mechanics. to hinder their performance. One must pay greater attention on this limitation as
Quantum computers share theoretical similarities with non-deterministic and probabilistic computers. This is similar to the ability to be in more than one state simultaneously. It may be noted that the field of quantum computing was first introduced by Richard Feynman in 1982 [22]. The Nobel prize-winning physicist Richard Feynman thought of the idea of a 'quantum computer', a computer that uses the effects of quantum mechanics to its advantage as early as in 1982 [22]. For quite good length of time, the notion of a quantum computer was primarily of theoretical interest only. In the recent times quantum computers have received more attention. This interest may also be due to the invention of an algorithm to factor large numbers, on a quantum computer, by Peter Shor (Bell Laboratories). By the use of this algorithm, quantum computer is able to crack codes much more quickly than any ordinary computer. It is reported that quantum computer is capable of performing Shor's algorithm [24] and is able to break current cryptography techniques in a matter of seconds.

It is expected that Quantum computers will someday replace silicon chips, just like the transistor replaced the vacuum tube. It seems at the moment the technology required to develop such a quantum computer may take sufficiently long time. In fact most research in quantum computing remained theoretical. The most advanced quantum computers have not gone beyond manipulating more than 16 qubits,; meaning that they are a far away from practical applications. But is expected that someday the

quantum computers could perform faster calculations, which are time-consuming on conventional computers. Many advancements have been made in quantum computing in the last few years. We would learn of some of the developments in research on quantum computers.

In 1998 Los Alamos and MIT researchers managed to spread a single qubit across three nuclear spins in each molecule of a liquid solution of alkaline (an amino acid used to analyze quantum state or trichloro-ethylene (a chlorinated hydrocarbon used for quantum error correction) molecules. Investigators used the idea of entanglement, to study interactions between states as an indirect method for analyzing the quantum information.

The quantum computer uses nuclear magnetic resonance (NMR) to manipulate particles in the atomic nuclei of molecules of trans-crotonic acid, a simple fluid consisting of molecules made up of six hydrogen and four carbon atoms. The NMR is used to apply electromagnetic pulses, which force the particles to line up. These particles in positions parallel or counter to the magnetic field allow the quantum computer to mimic the information-encoding of bits in digital computers. This work was carried out in 2000 March. The scientists at Los Alamos National Laboratory announced the development of a 7-qubit quantum computer within a single drop of liquid.

In August 2000 [47], the 5-qubit quantum computer was designed to allow the nuclei of five fluorine atoms to interact with each other as qubits and can be programmed by radio frequency pulses and be detected by NMR instruments similar to those used in hospitals. Led by Dr. Isaac Chuang, the IBM team was able to solve in one step a mathematical problem that would take conventional computers repeated cycles. The problem of order-finding, involved finding the period of a particular function, a typical aspect of many mathematical problems related to cryptography.

Shor's Algorithm is a method for finding the prime factors of numbers (which plays an intrinsic role in cryptography). The scientists of IBM in 2001 used a 7-qubit computer to find the factors of 15 [24]. The computer correctly deduced that the prime factors were 3 and 5.

The scientists at the Institute of Optics in 2005, created the first **qubyte** or series of 8 qubits, using ion traps.

In 2006 Scientists in Waterloo and Massachusetts devised methods for quantum control on a 12-qubit system and Quantum control becomes more complex as systems employ more qubits.

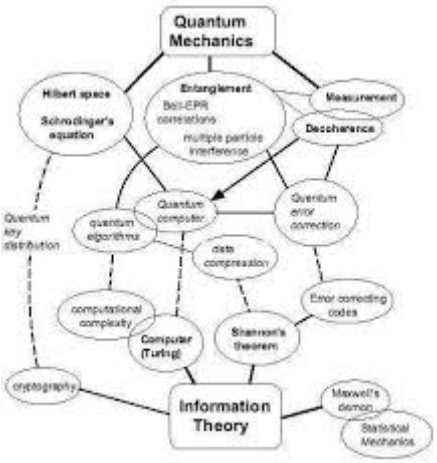
The computer developed in 2007 by D-Wave demonstrated a 16-qubit quantum computer which is used to solve Sudoku puzzle and other pattern matching problems. The D - Wave Company claimed to produce practical systems by 2008. But some of the pessimists believed that the practical quantum computers are still decades away. Also the system designed by D-Wave is not scale-able, and that many of the claims on D-Wave's Web site are simply impossible. The name quantum comes due to quantum mechanics in its inner workings. So the name is not from the problems it is solving, but how it is solving them.

There are several limitations on the computers. What they can and cannot depend on the laws of physics that governs them. The truely fundamental laws of the universe are still not known.

The use of Deutschian [24] closed time like curve (D-CTC) is a form of time travel that (at least naively) appears to be allowed by general relativity. David Deutsch [18] suggested a version of these that preserves causality (think 12 monkeys - you can travel in time, but you can't actually alter the past). Scott Aaronson and John Watrous [2, 45] wrote an interesting paper discussing the type of problems a computer built with D - CTC could solve efficiently. It's fascinating to see the interaction between computer science and the frontier of physics.

The contemporary way of 'generating', QC is to take probabilistic computing, which allows complex-valued probabilities, and require that the L- 2 norm [55] of the probabilities sums to 1 rather than the L-1 norm.

It is believed that if a functional quantum computers can be built, it may be valuable in factoring large numbers. This may be extremely useful for decoding and encoding secret information. Further such a system designed may bring revolutionary changes like, no information on the Internet would remain safe. The currently available encryption procedures are simple, compared to the complicated methods of quantum computers. It is thought that Quantum computers could also be used to search large databases in a fraction of conventional computer time. It is expected that quantum computers can be used to study several issues related to quantum mechanics.
It is well-known that quantum computing is still in its early stages of development. Many scientists believe that the technology needed to create a practical quantum computer may take sufficiently long time as Quantum computers must have at least several dozen qubits to be able to solve real-world problems.



4. Fundamental Aspects:

A quantum computer maintains a sequence of qubits. A single qubit can represent a one, a zero, or any quantum superposition of those two qubit states. A pair of qubits can be in any quantum superposition of 4 states, and three qubits in any superposition of 8 states. In general, a quantum computer with n qubits can be in an arbitrary superposition of up to 2^n different states simultaneously. This compares to a normal computer that can only be in one of these 2n states at any one time.

A qubit or quantum bit is a unit of quantum information - the quantum analogue of the classical bit. A qubit is a two-state quantum-mechanical system, such as the polarization of a single photon where the two states are vertical polarization and horizontal polarization. In a classical system, a bit would have to be in one state or the other. However quantum mechanics allows the qubit to be in a superposition of both states at the same time, a property which is fundamental to quantum computing.
The concept of the qubit was unknowingly introduced by Stephen Wiesner in 1983, in his proposal for un-forgeable quantum money, which he had tried to publish for over a decade.
The coining of the term "qubit" is attributed to Benjamin Schumacher [46]. In the acknowledgments of his work, Schumacher states that the term qubit was invented in jest due to its phonological resemblance with an ancient unit of length called cubit, during a conversation with William Wootters. He described a way of compressing states emitted by a quantum source of information so that they require fewer physical resources to store. This procedure is now known as Schumacher compression.
The bit is the basic unit of information. It is used to represent information by computers. Irrespective of the physical realization, a bit has two possible states typically thought of as 0 and 1, but more generally - and according to applications - interpretable as true and false, night and day, or any other dichotomous choice. An analogy to this is a light switch - it's off

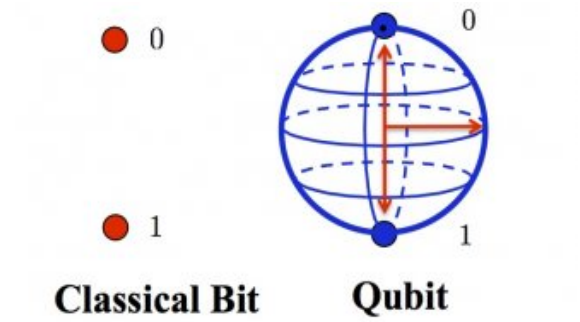
position can be thought of as 0 and it's on position as 1.

A qubit has a few similarities to a classical bit, but is overall very different. There are two possible outcomes for the measurement of a qubit—usually 0 and 1, like a bit. The difference is that whereas the state of a bit is either 0 or 1, the state of a qubit can also be a superposition of both [47]. It is possible to fully encode one bit in one qubit. However a qubit can hold even more information, for example up to two bits using Super-dense coding.

The two states in which a qubit may be measured are known as basis states (or basis vectors). As is the tradition with any sort of quantum states, they are represented by Dirac - or "bra–ket"- notation. This means that the two computational basis states are conventionally written as $|0\rangle$ and $|1\rangle$ (pronounced "ket 0" and "ket 1").

Qubit states: A quantum computer operates by setting the qubits in a controlled initial state that represents the problem at hand and by manipulating those qubits with a fixed sequence of quantum logic gates. The sequence of gates to be applied is called a quantum algorithm. The calculation ends with a measurement, collapsing the system of qubits into one of the 2^n pure states, where each qubit is zero or one. The outcome can therefore be at the most n classical bits of information. Quantum algorithms are often non-deterministic, in that they provide the correct solution only with a some known probability.

Quantum computers replace traditional bits that are used in digital communications with quantum bits, or qubits. Potential applications can be found in a variety of fields including medicine and space missions. Qubits exist in a state of superposition, meaning they can be in both states at once, rather than restricted to either binary state as traditional bits function.



One firm based at Cambridge believes that the software will aid the commercialization of the emerging technology further, facilitating users in controlling the operations a quantum computer can perform.

QUBIT CONTROL: Microscopic particles can be programmed to control qubits in quantum computers by using control devices. Ion traps use optical or magnetic fields (or a combination of both) to trap ions. Optical traps use light waves to trap and control particles. Quantum dots, made of semiconductor material and are used to manipulate electrons. Semiconductor impurities containing electrons are controlled by using "unwanted" atoms found in semiconductor material. Superconducting circuits allow electrons to flow with almost no resistance at very low temperatures [53].

Each qubit can assumes a wide range of values, and a moderate number of them can hold an insane quantity of information.

Just 100 qubits can store 1,267,650,600,228,229,401,496,703,205,375 different numbers - many trillion times the storage capacity of all computers ever made. In other words, 100 qubits can simultaneously represent all possible 100-bit numbers in their huge quantum state, unlike classical 100-bit computer, which can represent just one.

This vast ability means that quantum computers can provide immense power, many times faster than any classical computer.

International Journal of Scientific Engineering and Applied Science (IJSEAS) - Volume-1, Issue-6, September 2015
ISSN: 2395-3470
www.ijseas.com

5. Definition The Quantum Computer:

The Turing machine, developed by *Alan Turing* in the 1930s, is a theoretical device consisting of tape of unlimited length that is divided into small squares. Each square can either hold a symbol (1 or 0) or be left blank. A read-write device reads these symbols and blanks giving the machine its instructions to perform a certain program. In the case of a quantum turing machine the tape exists in a quantum state, as does the read-write head. This means that the symbols on the tape can be either 0 or 1 or a superposition of 0 and 1. In other words the symbols are both 0 and 1 and all points in between. While a normal Turing machine can only perform one calculation at a time, a quantum Turing machine can perform many calculations at one go.

Today's computers, like a Turing machine work by manipulating bits that exist in one of the two states a 0 or a 1. Quantum computers aren't limited to two states; they encode information as quantum bits, or **qubits**, which can exist in superposition. Qubits represent atoms, ions, photons or electrons and their respective control devices that are working together to act as computer memory and a processor. A quantum computer has the potential to be millions of times more powerful than today's most powerful supercomputers due to multiple states. The superposition of qubits is what gives quantum computers their inherent parallelism. According to physicist David Deutsch [48**]**, this parallelism allows a quantum computer to work on a million computations at one go. A 30-qubit quantum computer would be equal to the processing power of a conventional computer that could run at 10 teraflops (i.e. trillions of floating-point operations per second). Today's typical desktop computers run at speeds measured in gigaflops (i.e. billions of floating-point operations per second).
Quantum computers also utilize another aspect of quantum mechanics known as entanglement [50**]**. One of the problems quantum computers is that if one tries to look at the sub-atomic particles, which could bump them, and thereby change their value. If he looks at a qubit in superposition to determine its value, the qubit will assume the value of either 0 or 1, but not both (similar to digital computer). In order to make a practical quantum computer, scientists have to devise ways of making measurements indirectly to preserve the system's integrity. Entanglement provides a potential answer. In quantum physics, if one applies an outside force to two atoms, it can cause them to become entangled, and the second atom can take on the properties of the first atom. So if left alone, an atom will spin in all directions. The instant it is disturbed it chooses one spin, or one value At the same time, the second entangled atom will choose an opposite spin, or value. This allows scientists to know the value of the qubits without actually looking at them.

6. Architecture:

A Layered framework for the quantum computer Architecture is given below.

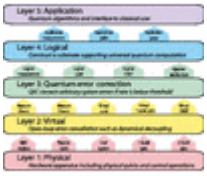


figure-1

A review of the progress that has been made in developing architectures of quantum computing, quantum computers is available [14, 53]. The highlight is the process of integrating the basic elements that have already been developed, and introducing the challenges remain in delivering on the promise of quantum computing.
The most famous development to date in quantum algorithms is Shor's algorithm for factoring large numbers in polynomial time. While the vernacular press often talks of factoring large numbers "in seconds", using a quantum computer. But in reality it is not possible to discuss the prospective performance of a system without knowing the physical and

logical clock speed. The topology of the interconnect among the elements; the number of logical quantum bits (qubits) is available in the system, and the details of the algorithmic implementation is given without specifying the architecture. Figure 1 illustrates the impact that architecture can have on the bottom-line viability of a quantum computer. The architecture used can make the difference between an interesting and an immediate threat to all RSA (due to Ron Rivest, Adi Shamir, and Leonard Adleman) encryption processes.

In developing a quantum computer architecture we have much to learn from classical computer architecture,. Foremost among these caveats is that the delicate nature of quantum information demands that memory elements be very active. Second, long wires or long-distance connections inside a quantum computer are either nonexistent, requiring nearest neighbor, cellular automaton-like transfer of data, or are at best poor quality, requiring much effort to transfer even a single qubit from place to place, using quantum teleportation and error management techniques. Thus, the principles of classical computer architecture can be applied, but the answers arrived at will differ from classical architectures.

Quantum computer architecture as a field remains in its infancy, but carries much promise for producing machines that vastly exceed current classical capabilities, for certain systems designed to solve certain problems. As we begin to design larger quantum computers, it must be recognized that large systems are not simply larger versions of small systems. The conceptual stack of subfields that must all contribute to a scalable, real-world machine is divided into a set of layers where in the elements of this structure in turn, all leading to the central core of quantum computer architecture have been discussed.

At the bottom of the stack we have the technologies for storing individual qubits, and processing or transporting them to take part in a larger computation. How small groups of qubits will interconnect is the first problem quantum computer architecture must solve. Given the fragility of quantum data, how many qubits be kept "alive" long enough to complete a complex computation? The solution to this problem is the field of quantum error correction (QEC), began with studies demonstrating that arbitrarily accurate computation is theoretically possible even with imperfect systems, but our concern here is the design of subsystems for executing QEC, which can be called the quantum computer micro- architecture. Recent progress in experimentally demonstrated in building blocks and the implementation of QEC which are the first two topics addressed in this article.

At the top of the stack, machines will be designed for specific workloads, to run certain algorithms that exist and computational complexity classes are believed to be inaccessible to classical computers. Without these algorithms, there will be no economic incentive to build and deploy machines.

With context established at both the top and bottom of the stack, the progress that has been made toward integrated architectures, and a detailed example of the immense scale-up in size and slowdown in speed arising from the error correction needs of a full-scale investigation of digital quantum computer. We note that the process of writing this article has been made substantially easier by the appearance in the last few years of excellent reviews on architecture.

7. Developments

There are a number of quantum computing models, distinguished by the basic elements in which the computation is decomposed. The four main models of practical importance are developed only in recent times.

a. The *quantum gate array* (computation decomposed into sequence of few-qubit quantum gates),
b. The *one-way quantum computer* (computation decomposed into sequence of one-qubit measurements applied to a

highly entangled initial state is called cluster state),

c. The *adiabatic quantum computer* (i.e. computation decomposed into a slow continuous transformation of an initial Hamiltonian into a final Hamiltonian, whose ground states contains the solution), and
d. The topological quantum computer (computation decomposed into the braiding of anyone in a 2D lattice).

The *Quantum Turing machine* is at theoretical level but direct implementation of this model is yet to receive sufficient attention. All four models of computation proved to be equivalent to each other in the sense, that each can simulate the other with no more than polynomial overhead. Of course many researchers are pursuing practical implementing a quantum computer\ using the models mentioned (depending on the physical system used to realize the qubits):

a. Superconductor-based quantum computers (including SQUID-based quantum computers) qubit implemented by the state of small superconducting circuits (Josephson junctions).
b. Trapped ion quantum computer (qubit implemented by the internal state of trapped ions),
c. Optical lattices (qubit implemented by internal states of neutral atoms trapped in an optical lattice), electrically defined or self-assembled quantum dots (see Loss-DiVincenzo quantum computer), where in qubit given by the spin states of an electron is trapped in the quantum dot),
d. Quantum dot charge is based on semiconductor quantum computer (qubit is the position of an electron inside a double quantum dot).
e. Nuclear magnetic resonance on molecules in solution is a liquid-state NMR (qubit is provided by nuclear spins within the dissolved molecule),
f. Solid-state NMR Kane quantum computers (qubit realized by the nuclear spin state of phosphorus donors in silicon),
g. Electrons-on-helium quantum computers (qubit is the electron spin),
h. Cavity quantum electrodynamics (CQED) (qubit provided by the internal state of atoms trapped in coupled high-finesse cavities),
i. Molecular magnet Fullerene-based ESR quantum computer (where in qubit is based on the electronic spin of atoms or molecules encased in fullerene structures),
j. Optics-based quantum computer called Quantum optics (qubits realized by appropriate states of different modes of the electromagnetic field),
k. Diamond-based quantum computer (in which qubit is realized by the electronic or nuclear spin of Nitrogen-vacancy centers in diamond),
l. Bose–Einstein condensate-based quantum computer.
m. Transistor-based quantum computer – string quantum computers with entrainment of positive holes using an electrostatic trap,
n. Rare-earth-metal-ion-doped inorganic crystal based quantum computers (qubit realized by the internal electronic state of dopants in optical fibers),
o. The large number of candidates demonstrates that the topic, in spite of rapid progress, is still in its infancy. But at the same time, there is also a vast amount of flexibility.

In 2005, researchers at Michigan built a semiconductor chip that functioned as an ion trap. Such devices, produced by standard lithography techniques, may point the way to scalable quantum computing tools. An improved version was prepared in 2006.

In 2009, researchers at Yale University created the first rudimentary solid-state quantum processor. The two-qubit superconducting chip

was able to run elementary algorithms. Each of the two artificial atoms (or qubits) were made up of a billion aluminum atoms but they acted like a single one that could occupy two different energy states.

Another team, working at the University of Bristol, also created a silicon-based quantum computing chip, based on quantum optics. The team was able to run Shor's algorithm on the chip. Further developments were made in 2010. Springer publishes a journal ("Quantum Information Processing") devoted to the subject.

In April 2011, a team of scientists from Australia and Japan have finally made a breakthrough in quantum called teleportation. They have successfully transferred a complex set of quantum data with full transmission integrity achieved. Also if the qubits are destroyed in one place, but instantaneously resurrected in another, without affecting their super-positions.

Photograph of a chip constructed by D-Wave Systems Inc., mounted on wire-bonded in a sample holder. The D-Wave processor is designed to use 128 superconducting logic elements that exhibit controllable and tunable coupling to perform operations.

In 2011, D-Wave Systems announced the first commercial quantum annealer on the market by the name D-Wave One. The company claims that this system uses a 128 qubit processor chipset. In May 2011 D-Wave announced that Lockheed Martin Corporation entered into an agreement to purchase a D-Wave-1 system. Lockheed Martin and the University of Southern California (USC). An agreement was made to house the D-Wave- One Adiabatic Quantum Computer at the newly formed USC Lockheed Martin Quantum Computing Center, part of USC's Information Sciences Institute campus in Marina del Rey.

During the same year, researchers working at the University of Bristol created an all-bulk optics system which is able to run an iterative version of Shor's algorithm. They successfully managed to factorize 21.

In September 2011 researchers also proved that a quantum computer can be made with Von Neumann architecture (separation of RAM).

In 2012 IBM scientists said that they have made several breakthroughs in quantum computing that put them "on the cusp of building systems that will take computing to a whole new level."

In April 2012 a multinational team of researchers from the University of Southern California, Delft University of Technology, the Iowa State University of Science and Technology, and the University of California, Santa Barbara, constructed a two-qubit quantum computer on a crystal of diamond doped with some manner of impurity, that can easily be scaled up in size and functionality at room temperature. Two logical qubit directions of electron spin and nitrogen kernels spin were used. A system which formed an impulse of microwave radiation of certain duration and the form was developed for the maintenance of protection against de-coherence. By means of this computer Grover's algorithm for four variants of search has generated the right answer from the first trial in 95% of cases.

8. Quantum Information And Quantum Computing:

The research effort of exploring the consequences of quantum mechanics for information and computation began with Feynman's 1982 [22], proposal to build a computer that takes advantage of quantum

mechanics has grown enormously since Peter Shor's 1994 [24] quantum factoring algorithm. Extensive experimental and theoretical research efforts to build a quantum computer, have been responsible in investigations related to quantum information and quantum computing

Quantum Algorithms and Complexity: If a perfectly functioning quantum computer were built, which problems could it solve faster than conventional computers, and which problems do not admit any speedup? It studies complexity classes defined using quantum computers and quantum information which are computational models based on quantum mechanics. It studies the hardness of problems in relation to these complexity classes, and the relationship between quantum complexity classes and classical (i.e., non-quantum) complexity classes.

A complexity class is a collection of problems which can be solved by some computational model under resource constraints. For instance, the complexity class P is defined to be the set of problems solvable by a Turing machine in polynomial time. Similarly, one may define a quantum complexity class using a quantum model of computation,. Thus, the complexity class BQP is defined to be the set of problems solvable by a quantum computer in polynomial time with bounded error.

Two important quantum complexity classes are BQP and QMA which are the bounded-error quantum analogues of P and NP. One of the main aims of quantum complexity theory is to find out where these classes lie with respect to classical complexity classes such as P, NP, PP, PSPACE and other complexity classes.

Shor's algorithm, named after mathematician Peter Shor, [24] is a quantum algorithm (an algorithm that runs on a quantum computer) for integer factorization formulated in 1994. It solves the following problem: Given an integer N, find its prime factors.

On a quantum computer, to factor an integer N, Shor's algorithm runs in polynomial time (the time taken is polynomial in log N, which is the size of the input). Specifically it takes time and quantum gates of order

$O((\log N)^2(\log\log N)(\log\log\log N))$

using fast multiplication, demonstrating that the integer factorization problem can be efficiently solved on a quantum computer and is thus in the complexity class is in BQP. This is substantially faster than the most efficient known classical factoring algorithm, the general number field sieve, which works in sub-exponential time is about

$O(e^{1.9 (\log N)1/3 (\log\log N)2/3})$.

The efficiency of Shor's algorithm is due to the efficiency of the quantum Fourier transform, and modular exponentiation by repeated squaring.

Quantum Information theory: How can we communicate and compute using quantum information in the presence of noise? What are the properties of entanglement?

Measurement and Control: How can quantum information be useful in applications apart from computers and communication devices, such as clocks and precision measurements?

Applications and Connections: How can ideas from QI / QC contribute to areas as diverse as convex optimization, black holes and condensed-matter physics? Quantum Information and Quantum Computing Theory (QI & QC) research at Center for Theoretical Research (CTR) of MIT.

Some of the notable contributions of theoretical physics group include the Quantum Adiabatic Algorithm and Quantum Walk Algorithms. Efficient protocols for simulating quantum channels (Harrow, Shor) and algorithms and hardness results for testing entanglement (Harrow) [52] have been carried out. An ongoing research at MIT in QI & QC includes work on new quantum algorithms, efficient simulations of quantum systems, connections to convex optimization, understanding the role of de-coherence in excitonic transport (e.g. in photosynthesis) and many other topics. Some universities also included Quantum information

is included into the curriculum with a junior lab experiment on NMR quantum computing [56] .

9. Operating System

The first operating system for a quantum computer has been developed by researchers which is signal for a significant step towards creating a practical version of the ultra powerful machines. An operating system was developed by Cambridge Quantum Computing Lab (CQCL), using a proprietary custom designed high speed supercomputer which accurately simulates a quantum processor.

The development of new OS "t | ket > " is a major milestone. This OS has been facilitated by CQCL's own proprietary custom designed high-speed super computer and this allowed the company to accurately mimic how a quantum processor will work.
A quantum computer takes advantage of quantum interference. Consequently creating an immense advantage in improving computational speed over conventional computers. This is also capable of carrying out massive parallel computations simultaneously. It has significant applications for the global economy, including financial markets, insurance, intelligence, cyber-security, internet, medicinal and pharmaceutical research, defense, energy, database management, logistics and communications.

Quantum computing may be a reality much earlier than originally anticipated. It will have profound and far-reaching effects on a vast number of aspects of our daily lives. It is expected that Quantum computers may be holding revolutionary potential in a variety of fields due to their immense processing power. Governments, companies and organizations are currently developing the technology in the belief that it could be the future of computing.

Working QC is getting closer: Even though it can be extremely expensive, Quantum computing has been coming on leaps and bounds. The speed with which it completes complex tasks when compared to regular PCs is one of the biggest advantages it brings. The working of quantum computer means accomplishing simultaneous error detection of two quantum errors.

Researchers are working on significant activities to develop quantum computing technology that might enable the development of a Superfast quantum computer, though there has been less work done in the development of an Operating System that might control the quantum computers. It will have profound and far-reaching effects on a vast number of aspects of our daily lives. In the course of Polishing Quantum Computing CQCL's new operating system for the quantum computer comes almost at the same time along with IBM; who brought us even closer to a working with Superfast quantum computer by discovering a new method for correcting two errors that a quantum computer can make.

One of the biggest issues that prevent us from developing Superfast Quantum Computers is — Quantum computing is greatly fragile. Even the slightest fault can cause a major error to the computer. However, IBM researchers have discovered a new way to detect both types of quantum computer errors, and revealed a new, square quantum bit circuit design. IBM said it can be easily scaled up to make high-performance computers, according to the details published in Nature Communications.

Traditional computers use the "bits" to represent information as a 0 or a 1; therefore they are so much slower. On the other hand, Quantum computers use "qubits" (quantum bits) to represent information as a 0, 1, or both at the same time. The major problem with qubits is that they sometimes flip without warning.

Qubits can suddenly flip from 0 to 1, which is called a bit flip, or from 0+1 to 0-1, which is called a phase flip. These flips are the actual

culprits that create all kinds of errors. IBM's quantum circuit, consisting of four superconducting qubits on a one-quarter inch square chip, allowing investigators to detect bit-flip as well as phase-flip quantum errors simultaneously.
http://thehackernews.com/2015/05/os-quantum-computing.html#sthash.ovzDVYk1.dpuf.

10.Comparison With Other Technologies

Quantum Computing promises extraordinary computational speed for special class of problems. Like DNA computing, quantum computing is suitable for problems that require massive parallel processing.

Qubit is the equivalent of a bit in classical computers. Two qubits can represent the information in four different states, namely 00, 01, 10 and 11. The difference from the classical computer becomes apparent when it comes to processing information. In a classical computer one would need to enter these states to the digital system to get outputs one by one. In a quantum computer, all states enter the system simultaneously and all outputs are generated at the same time i.e. simultaneously. The outputs generated are in a superposed state and all available at the same time.

The power of quantum computing becomes apparent when one considers large number of input qubits. Quantum gates can be connected back to back and turned on and off to implement complicated operations**.** Currently, there are only few problems that can take advantage of the massive parallelism of quantum computers. Computing with quantum computers require initialization, processing and reading of cubits. Currently there are more than one way of realizing cubits in hardware and this is likely to increase in the near future.

The currently available speed of a spin cubit gate made in silicon structure is in the order of 102 sec. and external operations dealing with cubits require 105 sec. Linear density of cubits in semiconductors is currently 65 nm 14. Although the speed does not seem very impressive, considering the inherent parallelism of each cubit gate, the overall processing speed is likely to be very high.

11. Future Of Quantum Computing

It may be noted that, IBM has made greater progress with its simultaneous error detection to make a working quantum computer will be a reality in near future . CQC gave a report that the developments could affect our lives in a larger way when quantum computing will be a reality [47].

The massive amount of processing power generated by computer manufacturers and algorithms developers has not yet been able to quench our thirst for speed and computing capacity. In 1947, Computer engineer **Howard Aiken** said that just six electronic digital computers would satisfy the computing needs of the United States. Some authors have made similar predictions about the amount of computing power that would support our growing technological needs. It is reported that Aiken didn't count on the large amounts of data generated by scientific research, the proliferation of personal computers or the emergence of the Internet, which have only fueled our need for more and more computing power.

The number of transistors on a microprocessor continues to double every 18 months. By the year 2020, we may find the circuits on a microprocessor which can be measured on an atomic scale. The next step will be to create to quantum computers is that they will harness the power of atoms and molecules to perform memory and processing tasks.

Quantum computers are expected to have the potential to perform certain calculations significantly faster, than any silicon-based computer. We know that computers have been around for the majority of the 20th century.

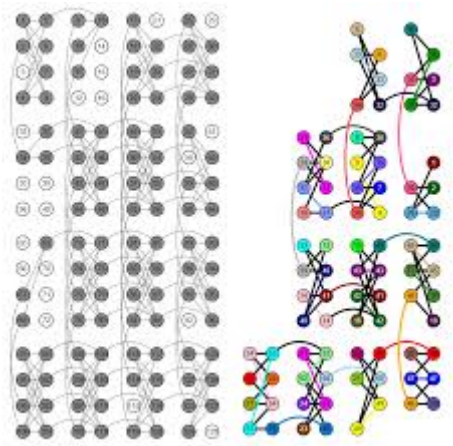
Quantum computing was first theorized in less than 30 years ago, by a physicist at the Argonne National Laboratory. Paul Benioff is credited with first applying quantum theory to computers in 1981. Benioff theorized about creating a quantum Turing machine.

The performance and quantum nature of the D-Wave-2 processor continues to be a topic of discussion with every new data release, and the performance figures that Google released in January-2014.

The key question at the heart of the D-Wave is whether or not the system is actually performing *quantum* annealing. Theoretically, the D-Wave-2 processor could be a relatively good simulation of a quantum computer. It may be the best simulation ever built — but still, an approximation of what the real thing would offer is yet to be perceived. The only way to determine whether or not the D-Wave performs true quantum annealing is to find a test case in which the D-Wave-2 performs far more better than the classical computers.

The D-Wave - 2 is limited by what's called "sparse connectivity," as shown below.

It may be noted that while each sub-group of eight qubits is tightly linked to its adjacent partners, the blocks themselves connect in far fewer places. Thus the limitation on the performance of the quantum is annealed as it limits the number of states that the quantum computer can test. This is a separate problem from the number of qubits in the system (up to 509 out of a possible 512 in this machine) . It's an issue of how interconnected the 509 functional qubits are.



According to Google, this sparse connectivity that's allowing classical computers to keep pace with D-Wave's quantum system. The company writes that, "For each solver, there are problems for which the classical solver wins or at least achieves similar performance. But the inverse is also true. For each classical solver, there are problems for which the hardware does much better." There are 9 ways quantum computing will change everything:

Lev Grossman [53] says that D-Wave's machines are "so radical and strange, people are still trying to figure out what it's for and how to use it.".

We live in the commercial age of Big Data, burying ourselves in information. We search queries, genomes, credit-card purchases, phone records, retail transactions, social media, geological surveys, climate data, surveillance videos, movie recommendations and D-Wave just happens to be selling "a very shiny new shovel."

Technology will bring radical changes for the following areas, to name a few:

1. Safer airplanes—Lockheed Martin plans to use its D-Wave to test jet software that is currently too complex for classical computers. **2. Discover distant planets**—Quantum computers will be able to analyze the vast amount of data collected by telescopes and seek out Earth-like planets. **3. Win elections**—Campaigners will comb through reams of marketing information to best exploit individual

voter preferences. **4. Boost GDP**—Hyper-personalized advertising, based on quantum computation, will stimulate consumer spending. **5. Detect cancer earlier**—Computational models will help determine how diseases develop. **6. Help automobiles drive themselves**—Google is using a quantum computer to design software that can distinguish cars from landmarks. **7. Reduce weather-related deaths**—Precision forecasting will give people more time to take cover. **8. Cut back on travel time**—Sophisticated analysis of traffic patterns in the air and on the ground will forestall bottlenecks and snarls. **9. Develop more effective drugs**—By mapping amino acids, for example, or analyzing DNA-sequencing data, doctors will discover and design superior drug-based treatments.

Quantum computing uses strange subatomic behavior to exponentially speed up processing. It could be a revolution, or it could be wishful thinking. D- wave developers say that

Quantum computers could represent an enormous new source of computing power--it has the potential to solve problems that would take conventional computers centuries, with revolutionary consequences for fields ranging from cryptography to nanotechnology, pharmaceuticals to artificial intelligence.

Of course Michael Byrne [57], on his article on " The Near-Term Future Of Quantum Computing? Analog Simulations" also feels the progress in quantum computing is slow.

Physicists have performed quantum calculations on small handfuls of qubits, the quantum analog of the classical bit information carrier, but the real prize remains distant. There is a reason for this: a quantum computer is really hard to do as it has to do with the fragility of quantum information (qubits), which, once disturbed, become classical junk. It's a hardware challenge. **How do** you protect a qubit - a single particle in a superposition of different states - when it's very surroundings threaten to wipe it out? It's worse than that even, because wiping out one qubit means potentially wiping out the entire network of entangled qubits, nuking not just one unit of information but every parallel processing unit too.

The physicist Ivan Deutsch has the task for the past 20 years in designing the guts of a quantum computer. In a great *Quanta* Q&A he offered some hope in the form of old-school computing: quantum simulations, not quite the real deal, but immensely powerful nonetheless.

The key component is what Deutsch [19] calls the "qubit." It's a complete atom rather than a single electron or other fundamental particle. It operates in a sort of fake or simulated quantum superposition in which it's allowed to occupy one of 16 different states, represented by energy levels. Deutsch explanation using a full atom of 16 possibilities is a fundamentally different than a computer using the classical bit (on or off) or the quantum qubit (on and off).

12. Limitations And Challenges For Quantum Simulators:

The evolution of the analog simulation is not digitized and the software cannot correct the tiny errors which accumulate during the calculation so we should error-correct noise on a universal machine. The analog device must keep a quantum superposition intact long enough for the simulation to run its course without resorting to digital error correction. This is believed as a challenge for the analog approach to quantum simulation.

With only few resources available than labs at, IBM analog quantum simulators offer short-term progress to academic researchers. Proper digital quantum computing is still limited to about 10 qubits at a time. This is similar to a train set inside a train set inside of an actual train. As reported so far no quantum error-correcting algorithm exists for real-life scales. The distance is still large . " Deutsch offered, "I would love to see just one universal logical qubit that can be indefinitely be error corrected."

13. Conclusion:

The recently developed new semiconductor chip of IBM is bringing us one step closer to the development of a practical quantum computer. The chip integrated four qubits, the basis of quantum computing, in a two by two, 2-D grid. Qubits are the bits that can exist as a 1 & a 0 simultaneously (superposition state), offering quantum computers the possibility of making simultaneous calculations. Quantum computers to be developed may consist grids with hundreds or thousands of qubits working together in making calculations. IBM's chip is supposed to be unique in the sense that it allows for the recognition of both kinds of quantum errors known as: *bit flips* (when a qubit representing 0 changes to a 1, or vice versa) and *phase flips* (the distortion of the superposition state of a qubit).

In 2015 march, Scott Wilsonson [33] suggests that Quantum Computing Takes Step forward,
A quantum computer chip – (Julian Kelly/University of California, Santa Barbara)
Researchers at the University of California, Santa Barbara and Google have made a big leap toward realizing the goal of ultra-powerful quantum computers. Such devices could easily break many current encryptions ciphers, which, by proxy, could help calculate complex problems in minutes, rather than months.

The key to, and the power of, quantum computing springs from that same instability, however: by utilizing even more qubits in an error-correction scheme, valid results might be read from such computers, despite relatively high rates of de-coherence. Although the amount of errors experienced in most quantum computing devices far exceeds the scope of any conventional error correction mechanism, throwing more qubits at the problem is exactly the solution that Google has come up with.
Working with an array of five qubits to hold data, the team inserted an additional four qubits next to them to devote exclusively to error correction. The four error-correcting qubits are allowed to observe the data qubits and essentially check their accuracy. By doing so, the team was able to reduce the failure rate by a factor of 8.5, according to their article in Nature.

The difficultly is that simply observing a qubit to determine if it has “flipped” into an error state via Even with this improvement, viable quantum computing has a long way to go. Despite their success, the team was only able to use the qubits in the classical manner of conventional bits, not taking advantage of the superpositioning that is expected to provide the lion’s share of quantum computing benefits.
The quantum computer promises to deliver a new level of computational power. A whole new theory of computation being developed incorporates the strange effects of quantum mechanics and considers every physical object to be some kind of quantum computer. A quantum computer thus produced will have the theoretical capability of simulating any finite physical system and may even hold the key to creating an artificially intelligent computer.
The quantum computers power to perform calculations across a multitude of parallel universes gives it, ability to quickly perform tasks which classical computers will never be able to practically achieve.. Some algorithms have already been invented which are proving to have huge implications on the world of cryptography. This is due to the commonly used cryptography techniques. A spinoff of quantum computing and quantum communication will allow information to be sent with secretly.

One very important feature of electromagnetic signals is measurability. This makes easy to read all the parameters of a signal without introducing changes to it. This is the exact reason why almost all techniques are equipped with encryption. This protects transmitted information from being read or altered by a third party. The communicating parties don’t have another channel to talk, and cryptosystem developers brilliantly solved a very complicated problem as to, how to negotiate a secret encryption key when all communication might

be observed by others. The solution to this problem is the foundation for protection systems, and quantum computers might break it.

The names “Quantum computing” and “Quantum cryptography” are accurate. These systems are based on quantum effects like **superposition and entanglement** of micro-particles. Quantum computers raise and answer to new questions in the security field, primarily in cryptography. However research workers interested in quantum computing should continue to analyze and keep connected to active schools of excellence in quantum computing research. It is necessary to share the information time to time on the developments as this is a most challenging area.

14.References:

1. "12-qubits Reached In Quantum Information Quest." Science Daily, May 2006. http://www.sciencedaily.com/releases/2006/05/060508164700.htm
2. Aaronson, Scott. "Shtetl-Optimized." April 10, 2007. http://scottaaronson.com/blog
3. Bone, Simone and Matias Castro. "A Brief History of Quantum Computing." Imperial College, London, Department of Computing. 1997. http://www.doc.ic.ac.uk/~nd/surprise_97/journal/vol4/spb3/
4. Boyle, Alan. "A quantum leap in computing." MSNBC, May 18, 2000. http://www.msnbc.msn.com/id/3077363
5. "Center for Extreme Quantum Information Theory (XQIT), MIT." Tech. News, March 2007. http://www.technologynewsdaily.com/node/6280
6. Centre for Quantum Computer Technology http://www.qcaustralia.org/
7. Cory, D.G., et al. "Experimental Quantum Error Correction." American Physical Society, Physical Review Online Archive, September 1998. http://prola.aps.org/abstract/PRL/v81/i10/p2152_1
8. Grover, Lov K. "Quantum Computing." The Sciences, July/August 1999. http://cryptome.org/qc-grover.htm
9. Hogg, Tad. "An Overview of Quantum Computing." Quantum Computing and Phase Transitions in Combinatorial Search. Journal of Artificial Intelligence Research, 4, 91-128 (1996). http://www.cs.cmu.edu/afs/cs/project/jair/pub/volume4/ hogg96a-html/node6.html
10. "IBM's Test-Tube Quantum Computer Makes History." IBM Research, December 19, 2001. http://domino.watson.ibm.com/comm/pr.nsf/pages/ news.20011219_quantum.html
11. Institute for Quantum Computing. http://www.iqc.ca
12. Jonietz, Erika. "Quantum Calculation." Technology Review, July 2005. http://www.technologyreview.com/Infotech/14591
13. Maney, Kevin. "Beyond the PC: Atomic QC." USA Today. http://www.amd1.com/quantum_computers.html
14. "Quantum Computing." Stanford Encyclopedia of Philosophy, February 26, 2007. http://plato.stanford.edu/entries/qt-quantcomp
15. Qubit.org http://www.qubit.org
16. Simonite, Tom. "Flat 'ion trap' holds quantum computing promise." New Scientist Tech, July 2006. http://www.newscientisttech.com/article/ dn9502-flat-ion-trap-holds-quantum-computing-promise.html
17. Vance, Ashlee. "D-Wave qubits in the era of Quantum Computing." The Register, February 13, 2007.

http://www.theregister.co.uk/2007/02/13/dwave_quantum

18. West, Jacob. "The Quantum Computer." Computer Science at Cal Tech, April 28, 2000. http://www.cs.caltech.edu/~westside/quantum-intro.html.
19. David Deutsch; The Fabric of Reality: One of the few books currently covering the subject of quantum computing / cryptography – 1997, chapters 2 and 9 are more related to QC .
20. David Harel; Algorithemics – The spirit of computing – Includes the history of computing theory and details of encryption techniques-.1992, Addison Wesley.
21. Various papers on quantum computers, most needing an in-depth knowledge to understand. Technical papers on quantum computation http://feynman.stanford.edu/qcomp/artlist.html.
22. R. P. Feynman, Int. J. Theoretical. Phys. 21, 467 (1982).
23. J. Preskill, "Battling De-coherence: The Fault-Tolerant Quantum Computer," Physics Today, June (1999).
24. Shor, P. W., Algorithms for
25. quantum computation: Discrete logarithms and factoring, in Proceedings of the 35th Annual Symposium on Foundations of Computer Science, IEEE Computer Society Press (1994).

25.Nielsen, M., "Quantum Computing," (unpublished notes) (1999).

26. Michael A. Nielsen & Isaac L. Chuang, Quantum Computation and Quantum Information 10th Anniversary Edition, CAMBRIDGE UNIVERSITY PRESS Cambridge, New York, Melbourne,2010

26. J. Preskill, "Quantum Computing: Pro and Con," quant-ph/9705032 v3, 26 Aug 1997.

27. Chuang, I. L., Laflamme, R., Yamamoto, Y., "Decoherence and a Simple Quantum Computer," (1995).

28. D. Deutsch, A. Ekert, "Quantum Computation," Physics World, March (1998).

29. http://thehackernews.com/2015/05/os-quantum computing.html#sthash.ovzDVYk1.dpuf,

30. Peter w. Shor; Introduction to quantum algorithms, proceedings of the symposium on applied mathematics. 2000.

31. Physical realization of a quantum computer by Jani-Petri of Martikainen Jani- http://www.helsinki.fi/ ˜jamartik.

32. Isaac L. Chuang, Lieven M. K. Vandersypen[2], Xinlan Zhou[2], Debbie W. Leung & Seth Lloyd, Experimental realization of a quantum algorithm; Nature 393, 143-146 (14 May 1998) | doi:10.1038/30181; Received 21 January 1998; Accepted 18 March 1998.

33. Scott Wilsonon, Quantum Computing Takes another Step Forward, March 09, 2015.

34.Joel Hruska ; D-Wave, disentangled: Google explains the present and future of quantum computing, quantum information on Extreme tech , on February 26, 2014.

35. Simon, D.R. (1994), "On the power of quantum computation", *Foundations of Computer Science, 1994 Proceedings. 35th Annual Symposium on*: 116–123.

36. Arthur O. Pittenge , An Introduction to Quantum Computing Algorithms, ; Springer science, 1999.

37 Approaching Quantum Computing, By Marinescu Dan C.; Pearson education , 2009

38. Introduction to Quantum Information Science, Vlatko Vedral, OUP Oxford, 28-Sep-2006 - Technology & Engineering -194 pages.

39. Ergodic Theory: Probability and Ergodic Theory Workshops, February 15-18 – edited by Idris Assan.

40. Quantum Turing Machines, Discussion Paper on MATHEMATICS, Encyclopedia of mathematics, The European Mathematical Society, Springer, 2010.

41. Deutsch, Davis; Quantum Theory, The Church Turing Principle and Universal Computer- Proceedings of the Royal society A 400 (1818) pp 97-107, 1985.

42. One complexity Theorists view of quantum Computing, TCS, 292 (3) (2003) pp 597-610.

43. Iriyama. S, Ohya , M. Volouvich, I. – Generalized Quantum Turing machine and it applications to sat chaos algorithm may 2004.

44. Yri Manim; Classical computing, quantum computing, and Shor's factoring algorithm, 1999

45. Scott Aaronson, John Watrous Closed time like curves make quantum and classical computing equivalent , Cornell Univ, august 2008.

46. Schumacher Benjamin; Who named qubit? , in Quantum Frontiers, Int. of quantum information and matter , June, 2015 .

47. Kevin Bonsor and Jonathan Strickland; How Quantum Computers Work, how-stuff- works

48. Qubits – Super position and Entanglement- A quantum Computer Tutor, 2003.

49. Quantum Entanglement – The free Encyclopedia- Wikipedia, 2015.

50. Van Meter Rodney ; State of Art in Quantum Computing Architecture , August – 2011.

51. Quantum Information and Quantum Computing

52. Aram W. Harrow, Anand Natarajan, and Xiaodi Wu; An improved semi-definite programming hierarchy for testing entanglement, MIT Center for Theoretical Physics,2014

53. Lev Grossman, Explains Quantum Computing, 2014.

54. Kevin Bonsor and Jonathan Strickland How Quantum Computers Work, Quantum Technologies Simplified, howstuffworks, 2015.

55. Aram W. Harrow, Avinatan Hassidim, Seth Lloyd; Quantum algorithm for solving linear systems of equations, Phys. Rev. Lett. vol. 15, no. 103, pp. 150502 (2009). .
56. Michael Byrne, Editor, The Near-Term Future of Quantum computing? Analog Simulations, 2015.