IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661, p- ISSN: 2278-8727Volume 15, Issue 1 (Sep. - Oct. 2013), PP 30-34
www.iosrjournals.org

Quantum communication and quantum computing

*Sweety Mittal, **Nilesh Kumar Dokania
Lecturar,Yaduvanshi college of engg and technology
Assistant Professor, Guru Nanak Institute Of Management

Abstract: *The subject of quantum computing brings together ideas from classical information theory, computer science, and quantum physics. This review aims to summarize not just quantum computing, but the whole subject of quantum information theory. Information can be identified as the most general thing which must propagate from a cause to an effect. It therefore has a fundamentally important role in the science of physics. However, the mathematical treatment of information, especially information processing, is quite recent, dating from the mid-20th century. This has meant that the full significance of information as a basic concept in physics is only now being discovered. This is especially true in quantum mechanics. The theory of quantum information and computing puts this significance on a firm footing, and has led to some profound and exciting new insights into the natural world. Among these are the use of quantum states to permit the secure transmission of classical information (quantum cryptography), the use of quantum entanglement to permit reliable transmission of quantum states (teleportation), the possibility of preserving quantum coherence in the presence of irreversible noise processes (quantum error correction), and the use of controlled quantum evolution for efficient computation (quantum computation). The common theme of all these insights is the use of quantum entanglement as a computational resource.*

Keywords: *quantum bits, quantum registers, quantum gates and quantum networks*

I. Introduction

First proposed in the 1970s, quantum computing relies on quantum physics by taking advantage of certain quantum physics properties of atoms or nuclei that allow them to work together as quantum bits, or qubits, to be the computer's processor and memory. By interacting with each other while being isolated from the external environment, qubits can perform certain calculations exponentially faster than conventional computers. . A quantum computer can do an arbitrary reversible classical computation on all the numbers simultaneously, which a binary system cannot do, and also has some ability to produce interference between various different numbers. By doing a computation on many different numbers at once, then interfering the results to get a single answer, a quantum computer has the potential to be much more powerful than a classical computer of the same size. In using only a single processing unit, a quantum computer can naturally perform myriad operations in parallel. Quantum computing is not well suited for tasks such as word processing and email, but it is ideal for tasks such as cryptography and modeling and indexing very large databases.

The review concludes with an outline of the main features of quantum information physics and avenues for future research.

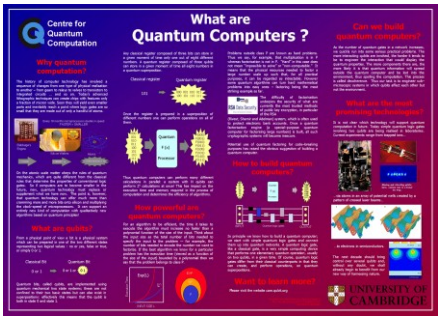

Fig 1. Basics of quantum computer

II. Requirements of hardware:

Storage: We'll need to store Qbits long enough to perform an interesting computation
Isolation: The Obits must be well isolated from the environment to minimize the decoherece effect.
Readout: We'll need to measure the Qbits efficiently and reliably.
Gates: We'll need to manipulate the quantum states of individual Qbit, so that we can perform quantum gates.

Precision: The quantum gates should be implemented with highly precision if we want the device to work properly.
Ion Trap: This idea has been suggested by Ignacio Cirac and Peter Zoller. In this scheme the Qbit is represented by a single ion held in linear Paul trap.
Cavity QED: Pellizzari, Cardiner, Cirac and Zoller have suggested that several neutral atoms to be stored in a small high finesse optical cavity. The quantum information can be stored in the internal states of the atoms
NMR: This scheme uses nuclear magnetic resonance technology and the Qbits are carried by a a certain nuclear spin in a particular molecule.

2.2 Algorithm

We describe a quantum algorithm that generalizes the quantum linear system algorithm to arbitrary problem specifications. We develop a state preparation routine that can initialize generic states, show how simple ancilla measurements can be used to calculate many quantities of interest, and integrate a quantum-compatible preconditioner that greatly expands the number of problems that can achieve exponential speedup over classical linear systems solvers. To demonstrate the algorithm's applicability, we show how it can be used to compute the electromagnetic scattering cross section of an arbitrary target exponentially faster than the best classical algorithm.

2.3 Complexity

Quantum Hamiltonian complexity is an exciting area combining deep questions and techniques from both quantum complexity theory and condensed matter physics. The connection between these fields arises from the close relationship between their defining questions: the complexity of constraint satisfaction problems in complexity theory and the properties of ground states of local Hamiltonians in condensed matter theory.
quantum Hamiltonian complexity provides new approaches and techniques for tackling fundamental questions in condensed matter physics, in particular the classical simulation of quantum many body systems. The area law plays a central role in recent progress on using tensor network based techniques for simulating such systems. The goal of this semester long program is to bring together leading computer scientists, condensed matter physicists and mathematicians working on these questions, and to build upon the existing bridges and collaborations between them. One of the important priorities will be to help establish a common language between the three groups, so that key insights from all three areas can be pooled in tackling the outstanding issues at the heart of quantum Hamiltonian complexity

2.4 Quantum Cryptography

According to Quantum Mechanics, given the most precise description possible of how things are now, the most you can do is predict the probability that things will turn out one way or another. Many people (including, famously, Albert Einstein) found this a disturbing feature of the theory, which suggested to them that Quantum Mechanics was not the real theory of nature, and that we were missing something. However, in a pivotal paper in 1964, John Bell showed a way of processing measurement results from certain experiments so that there is a threshold value, a maximum value which can be obtained by models (known as Local Hidden Variable models) which describe all possible models of physics which obey two fundamental properties: the theories should not be capable of transmitting information faster than the speed of light, and measurement results should be predetermined. However, the way that Bell combined these measurement results also predicted that a Quantum Mechanical system would exceed this threshold value, i.e., one of those assumptions on the nature of the physical world must be false. This prediction has been confirmed by numerous experiments in the intervening years.

To most, this unpredicatability of measurement results would present a problem. However, cryptographers look to benefit from such features. Information is always represented by measurable physical properties, and if such properties exist then, their value can be predicted with certainty without in any way disturbing a system. This is just a description of a perfect eavesdropping. Conversely, if such properties do not exist prior to measurements, then there is nothing to eavesdrop on. Hence, measuring the so-called Bell Inequalities in an experiment provides a test of just how much a quantum transmission has been eavesdropped. Remarkably, this requires very little by way of assumptions about the protocols that are being followed - it doesn't matter what devices we are using, or if we even trust the person who manufactured the devices or not - provided a Bell inequality is violated, we can use the measurement results to communicate securely. This is known as Device Independent cryptography. These ideas were first applied to the classic task in cryptography; key distribution, although has since been applied in various other instances such as the expansion of a sequence of random numbers.

III. Working In Quantum Computing

3.1.1 How Computers Work

Computers function by storing data in a binary number format, which result in a series of 1s & 0s retained in electronic components such astransistors. each component of computer memory is called a bit and can be manipulated through the steps of Boolean logic so that the bits change, based upon the algorithms applied by the computer program, between the 1 and 0 modes (sometimes referred to as "on" and "off").

3.1.2 How a Quantum Computer Would Work

A quantum computer, on the other hand, would store information as either a 1, 0, or a quantum superposition of the two states. Such a "quantum bit," called a qubit, allows for far greater flexibility than the binary system.

Specifically, a quantum computer would be able to perform calculations on a far greater order of magnitude than traditional computers ... a concept which has serious concerns and applications in the realm of cryptography & encryption. Some fear that a successful & practical quantum computer would devastate the world's financial system by ripping through their computer security encryptions, which are based on factoring large numbers that literally cannot be cracked by traditional computers within the life span of the universe. A quantum computer, on the other hand, could factor the numbers in a reasonable period of time.

3.2 Architecture

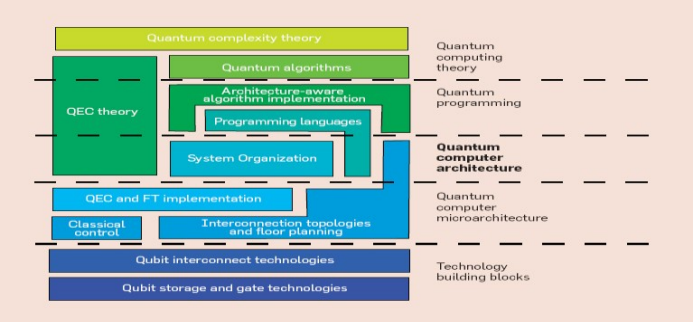

Fig2:Quantum Computing Sample Architecture

A sufficiently transparent architecture facilitates tool interoperability, focused point-tool development, and incremental improvements. Quantum algorithm designers and those developing quantum circuit optimizations can explore new algorithms and error-correction procedures in more realistic settings
involving actual noise and physical resource constraints. Researchers can also simulate important quantum algorithms on proposed new technologies before doing expensive lab experiments. Our four-phase design flow, shown in Figure , maps a high-level program representing a quantum algorithm
into a low-level set of machine instructions to be implemented on a physical device. The high-level quantum programming language encapsulates the mathematical abstractions of quantum mechanics and linear algebra.1 The design flow's first three phases are part of the quantum computer compiler (QCC). The last phase implements the algorithm on a quantum device or simulator.

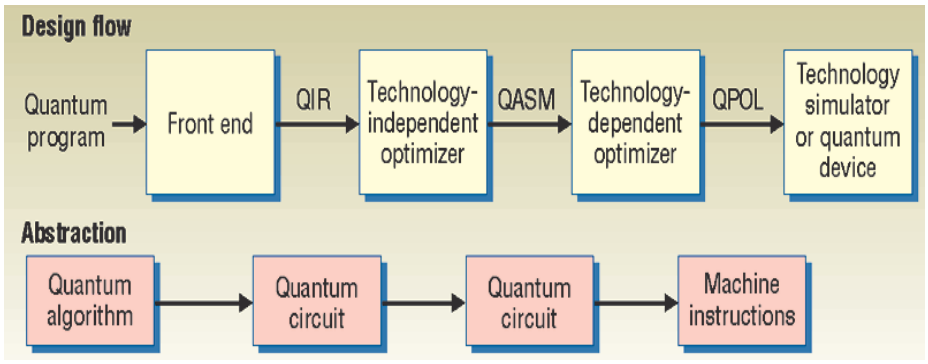

Fig3: Quantum Computing Layered Architeutre

4.1 Ongoing Research in Quantum Computing

Researchers in industry and government labs are exploring various aspects of quantum design and automation with a wide range of applications. In addition to the examples described below, universities in the US, Canada, Europe, Japan, and China are carrying out much broader efforts.

4.1.1 BBN Technologies

Based in Cambridge, Massachusetts, BBN Technologies (www.bbn.com) developed the world's first quantum key distribution (QKD) network with funding from the US Defense Advanced Research Projects Agency.The fiber-optical DARPA Quantum Network offers 24x7 quantum cryptography to secure standard Internet traffic such as Web browsing, e-commerce, and streaming video.

4.1.2 D-Wave Systems

Located in Vancouver, British Columbia, Canada, D-Wave Systems (www.dwavesys.com) builds superconductor-based software-programmable custom integrated circuits for quantum optimization algorithms and quantum-physical simulations. These ICs form the heart of a quantum computing system designed to deliver massively more powerful and faster performance for cryptanalysis,logistics,bioinformatics,and other applications.

4.1.3 Hewlett-Packard

The Quantum Science Research Group at HP Labs in Palo Alto,California,is exploring nanoscale quantum optics for information- processing applications (www.hpl.hp.com/research/qsr). In addition, the Quantum Information Processing Group at the company's research facility in Bristol, UK, is studying quantum computation, cryptography, and teleportation and communication (www.hpl.hp. com/research/qip).

4.1.4 Hypres

Located in Elmsford, New York, Hypres Inc. (www.hypres.com) is the leading developer of superconducting digital for wireless and optical communication. Based on rapid singleflux quantum logic, these circuits have achieved gate speeds up to 770 GHz in the laboratory.

4.1.5 IBM Research

Scientists at IBM's Almaden Research Center in California and the T.J.Watson Research Center's Yorktown office in New York developed a nuclear magnetic resonance (NMR) quantum computer that factored 15 into 3 □ □ 5 (http://archives.cnn.com/ 2000/TECH/computing/08/15/quantum.reut). Researchers at the Watson facility and the Zurich Research Lab are also developing Josephson junction quantum devices (www. research.ibm. com/ss_computing) as well as studying quantum information theory (www.research.ibm.com/quantuminfo).

4.1.6 Id Quantique

Based in Geneva, Switzerland, id Quantique (www.idquantique. com) is a leading provider of quantum cryptography solutions, including wire-speed link encryptors, QKD appliances, a turnkey service for securing communication transfers, and quantum random number generators.The company's optical instrumentation product portfolio includes single-photon counters and short-pulse laser sources.

4.1.7 Los Alamos National Lab

The Los Alamos National Lab (http://qso.lanl.gov/qc) in New Mexico is studying quantum-optical long-distance secure communications and QKD for satellite communications. It has also conducted groundbreaking work on quantum error correction, decoherence, quantum teleportation, and the adaptation of NMR technology to quantum information processing.

4.1.8 Magiq Technologies

MagiQ Technologies (www.magiqtech.com), headquartered in New York City, launched the world's first commercial quantum cryptography device in 2003. MagiQ Quantum Private Network systems incorporate QKD over metro-area fiberoptic links to protect against both cryptographic deciphering and industrial espionage.

4.1.9 NEC Labs

Scientists at NEC's Fundamental and Environmental Research Laboratories in Japan, in collaboration with the Riken Institute of Physical and Chemical Research, have demonstrated a basic quantum circuit in a solid-state quantum device (www.labs.nec.co.jp/Eng/innovative/E3/top.html). Recently, NEC researchers have also been involved in realizing the fastest fortnight-long, continuous quantum cryptography final-key generation.

4.1.10 NIST

Established in 2000, the Quantum Information Program at the US National Institute of Standards and Technology (http:// qubit.nist.gov) is building a prototype 10-qubit quantum processor— made of trapped ions, neutral atoms, or "artificial atoms" made of superconducting electrical circuits—to provide a proofin- principle of quantum information processing. Researchers at the program's facilities in Boulder,Colorado, and Gaithersburg, Maryland, are also developing a high-speed QKD system with
efficient and precise single-photon sources and detectors.

4.1.11 NTT Basic Research Labs

NTT's Superconducting Quantum Physics Research Group in Japan focuses on the development of quantum cryptography protocols (www.brl.ntt.co.jp/group/shitsuryo-g/qc). In particular, they have exhibited quantum cryptography using a single photon realized in a photonic network of optical fibers.

5.1 Future Outlook

At present, quantum computers and quantum information technology remains in its pioneering stage. At this very moment obstacles are being surmounted that will provide the knowledge needed to thrust quantum computers up to their rightful position as the fastest computational machines in existence. Error correction has made promising progress to date, nearing a point now where we may have the tools required to build a computer robust enough to adequately withstand the effects of decoherence. Quantum hardware, on the other hand, remains an emerging field, but the work done thus far suggests that it will only be a matter time before we have devices large enough to test Shor's and other quantum algorithms. Thereby, quantum computers will emerge as the superior computational devices at the very least, and perhaps one day make today's modern computer obsolete. Quantum computation has its origins in highly specialized fields of theoretical physics, but its future undoubtedly lies in the profound effect it will have on the lives of all mankind.

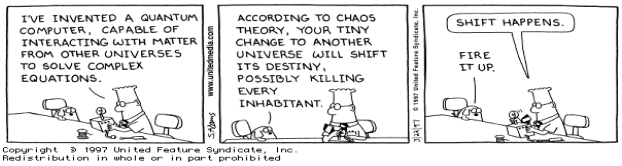

Fig 4

IV. Conclusion

The field of quantum computing is growing rapidly as many of today's leading computing groups, universities, colleges, and all the leading IT vendors are researching the topic. This pace is expected to increase as more research is turned into practical applications. Although practical machines lie years in the future, this formerly fanciful idea is gaining plausibility.

The current challenge is not to build a full quantum computer right away; instead to move away from the experiments in which we merely observe quantum phenomena to experiments in which we can control these phenomena. Systems in which information obeys the laws of quantum mechanics could far exceed the performance of any conventional computer. Therein lies the opportunity and the reward. No one can predict when we will build the first quantum computer; it could be this year, perhaps in the next 10 years, or centuries from now. Obviously, this mind-boggling level of computing power has enormous commercial, industrial, and scientific applications, but there are some significant technological and conceptual issue to resolve first.
But quantum computers will come.

References

[1] Jacob west http://www.cs.rice.edu/~taha/teaching/05F/210/news/2005_09_16.htm
[2] Jozef Gruska http://www.fi.muni.cz/usr/gruska/quantum/chapters.html
[3] ***Julian Voss-Andreae's "Quantum Objects*** http://physics.about.com/od/quantumphysics/f/quantumcomp.html
[4] Pearson IBM press http://www.ibmpressbooks.com/articles/article.asp?p=374693&seqNum=6
[5] Scott Aaronson MIT, Dave Bacon University of Washington https://www.google.co.in/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&ved=0CDIQFjAA&url=http%3A%2F%2Fwww.cra.org%2Fccc%2Ffiles%2Fdocs%2Finit%2FQuantum_Computing.pdf&ei=GuhcUuLKFsmArgfpuICQAg&usg=AFQjCNGr2Nl1e-w2s4j888JDZ7QD1-A9dA&sig2=9OCHbjLAddhd-QUzES9MCA
[6] Svore-aho-cross-chuang-markovhttp://research.microsoft.com/pubs/144689/qc-svore-aho-cross-chuang-markov-computer-magazine-article-a-layered-software-architecture-for-quantum-computing-design-tools-jan06-svore.pdf
[7] University of OXFORD http://www.maths.ox.ac.uk/groups/mathematical-physics/research-areas/quantum-information
[8] Webopedia http://www.webopedia.com/TERM/Q/quantum_computing.html