Quantum Information Technology

Ankita Sharma
Information Technology
Assistant Professor, JIMS, Rohini
New Delhi, India

Shraddha Kumar
Information Technology
Assistant Professor, JIMS, Rohini
New Delhi, India

***Abstract*— This paper deals with the subject of quantum computing bringing together ideas from classical information theory, computer science, and quantum physics. This paper not only gives a detail of quantum computing but the complete quantum information theory. It deals with the relationship among information theory and quantum mechanics. This term basically clubs quantum physics with information technology. Also if we think about the future taking in consideration the current research work going on in quantum information technology a new technology that is quantum information processing and communication (QIPC) could emerge. Now if we compare it with the information technology part we would require the information to be stored, stored, processed and communicated according to the laws of quantum physics in QIPC. This additional freedom could enable future QIT to perform tasks which can never be thought with ordinary IT.**

Keywords- QIPC, Qubit (Quantum bits), QIT.

I. INTRODUCTION

Information technology (IT) can be employed in two ways in quantum technology i.e. evolutionary and revolutionary. Both are potentially very important in their respective manner. If we talk in terms of the evolutionary work quantum physics is essentially employed as a tool, so it is possible to understand .On the other hand if we talk in terms of revolutionary work quantum mechanics is on the top. Now if we go into the depth of the evolutionary work for example, the development of smaller and faster silicon or in case of semiconducting devices we require to know the quantum behavior of the electrons. The superconducting benefits here would be faster digital switching and lower power consumption.

II. MOORE'S LAW AND BEYOND

In today's world many people are familiar with at least the consequences of Moore's Law – the fastest computer in the shops doubles in speed about every 18 months to two years. All this is happening because the size of the components is shrinking. As the size decreases the work efficiency increases. This exponential progress, first noted by Gordon Moore, a co-founder and former CEO of Intel, in 1965, has continued ever since [1] .But the problem is that this graph cannot run forever. The main hurdle will be faced with silicon, with oxide thinness, and other electronic devices because here a good amount of dollars will be required now if we talk about the Moore's second law, it tells us that the fabrication costs are also growing up exponentially. However, even if all the hurdles can be overcome, we will eventually run into nature.

Very small things do not behave the same way as big ones they begin to reveal their true quantum nature. Following Moore's Law, an extrapolation of the exponentially decaying number of electrons per elementary device on a chip gets to one electron per device around 2020. This is clearly too naive but it gives us a hint. Eventually we will get to scales where quantum phenomena rule, whether we like it or not. If we are unable to control these effects, then data bits in memory or processors will suffer errors from quantum fluctuations, and devices will fail. Clearly this alone makes a strong case for investment in research into quantum devices and quantum control. The results should enable us to push Moore's Law to the limit, evolving conventional information technology (IT) as far as it can go [2]. Instead of playing support act to make better conventional devices, let quantum mechanics take centre stage in new technology that stores, processes and communicates information according to the laws of quantum mechanics.

III. QUANTUM CRYPTOGRAPHY

In 1970 Stephen Wiesner had a inner realisation that quantum mechanics could be useful for cryptography and in 1984 Charles Bennett and Gilles Brassard proposed the well known BB84 scheme for quantum key distribution. After such discoveries many developments and new protocols have followed. This can be helped with an help of an example. The basic thought or basic idea is for Alice and Bob to share a secret key and to use this as a one-time-pad to communicate securely – quantum mechanics guarantees the security of the key. In BB84 Alice sends Bob some photons that are chosen randomly from the four states of two overlapping qubit (Quantum bits) bases (e.g. two orthogonal linear polarizations and right and left circular polarizations) and Bob has to measure in one of the two bases, chosen at random. After accumulating data, using public communication and sacrificing some of the bits, they can then identify what to keep (the raw key – when Bob used the correct basis), locate and correct errors, and scramble and reduce their correct bits (privacy amplification) to distil a shared secret key. Like Bob any eavesdropper has to measure the qubits – she has to play "guess the basis" and so cannot avoid introducing errors into the raw key. If Eve reads the lot, Alice and Bob know this and bin the raw key; if Eve reads only a fraction they can use the rest to distil some guaranteed secure bits. The development of quantum cryptography was motivated by the short-comings of classical cryptographic methods, which can be classified as either "public-key" or "secret-key" methods. Public-key encryption is based on the idea of a safe with two keys: a public key to lock the safe and a private key to open it (Ford, 2002; Ekert, 1995) [6]. Using this method, anyone can send a message since the public key is used to encrypt messages, but only someone with the private key can decrypt the messages. Public-key encryption, though secure at the moment, faces a serious threat as quantum computing comes closer to reality. Secret-key encryption requires that two users first develop and securely share a secret key, which is a long string of randomly-chosen bits. (Ekert, 1995). The users then use the secret key along with public algorithms to encrypt and decrypt messages. The algorithms are very complex, and can be designed such that every bit of output is dependent on every bit of input (Ford, 2002).

IV. Quantum computing

As we know irreversibility is what enables quantum cryptography, but on the other hand it may be taken as a hurdle for quantum computing. In a quantum computer, the fundamental unit of information (called a quantum bit or *qubit*), is not binary but rather more quaternary in nature. This qubit property arises as a direct consequence of its adherence to the laws of quantum mechanics which differ radically from the laws of classical physics [7]. A qubit can exist not only in a state corresponding to the logical state 0 or 1 as in a classical bit, but also in states corresponding to a blend or *superposition* of these classical states. In other words, a qubit can exist as a zero, a one, or simultaneously as both 0 and 1, with a numerical coefficient representing the probability for each state. This may seem counterintuitive because everyday phenomenon is governed by classical physics, not quantum mechanics -- which takes over at the atomic level. For example, if you keep opening the oven door to see what is happening, or the door does not fits in properly so heat leaks to the environment and the dish in the oven will not be baked properly. Quantum computing basically takes care of the superposition states evolving reversibly and generating entanglement between the many components of quantum machine. The 2^m possible states of an m-bit classical register form a suitable basis, so an m-qubit register can be placed in a superposition of all these states. This is why certain problems may be solved exponentially faster" by a quantum machine, in comparison to any classical machine. For a problem whose solution requires some property of the results of all 2^m different calculations, these have to be calculated separately in the classical case.

V. Examples

Now we will explain some examples i.e. list of things that can be done with the help of quantum computer.

Simulation: A quantum computer would be an excellent basic research tool. It is hard to squash a sizeable Hilbert space into ordinary memory, so simulating complex interacting quantum systems on a conventional computer is really hard work. Simulating them on an actual quantum machine would be much easier! Nuclear physicists, material scientists, molecular chemists and many others would queue up for time on a quantum computer, to investigate novel systems, regimes and materials inaccessible with classical modeling tools.

Searching and estimation: A classical search of a random list of M items to and a particular one requires the examination of at least M/2 of them to have a 50% success probability. Lov Grover has shown how a quantum search could find an item in only O ($M^{1/2}$) steps. In effect, using superposition states enables the examination of multiple items simultaneously. This speeds up the search, although in this case not exponentially. A similar square root improvement over classical algorithms for estimating the median of M data can be achieved in the quantum case [4].

Frequency standard: As the first working quantum machines will certainly consist of only a few interacting qubits, it would be nice to find something useful that can be done with such a simple system. A possibility is to use the ideas developed for quantum error correction in something other than a computer. A frequency standard effectively relies on the coherent oscillation of a pure atomic quantum state, so it is limited by decoherence as the atom/ion interacts with its environment.

VI. Experiments

Whereas quantum cryptography relies on the independent behavior of a string of non-interacting photon qubits, interactions between qubits are a must for quantum computation. There are a number of candidate systems currently being researched. There is no clear favorite as yet, to mirror the use of photons for cryptography. Those jostling for position are:

1. Ions/atoms in an electromagnetic trap, interacting through their quantum vibrational motion. Their internal energy levels form qubits can be coupled to these.

2. Cavity photon number states and atomic levels (Rydberg or optical) form qubits; external fields (microwave or optical) can be coupled in.

3. Electrons in quantum dots, interacting electrostatically or possibly magnetically. The discrete levels of the confined

electrons form qubits (or possibly qunits) and they couple readily to external fields.

4. Spin systems, interacting through their magnetic moments. These might be in a regular lattice, or, at a smaller scale, different spins within a large molecule, the so-called NMR quantum computing. A static external field separates out discrete spin levels for qubits. Time dependent fields can be applied to manipulate the system; in particular, in the NMR case the technology for doing this is very well developed.

5. Superconducting systems, interacting through the quantum motion of electric charges or magnetic flux. Such systems also have discrete levels and can be probed with external currents, voltages and fluxes.

VII. Conclusion

Quantum physics has the potential to generate both evolutionary and revolutionary developments in information technology. Expect evolutionary improvements to conventional logical processing to have shorter lead times than those for the emergence of radically new forms of processor. The intrinsic irreversibility of quantum measurement enables guaranteed secure communication. Quantum cryptosystems use secret keys, shared quantum mechanically, as one-time pads.

References

[1] K. K. Likharev, Physics World, vol. 10, no. 5, 39 (May 1997).
[2] A. Barenco, Contemporary Physics 37, 375 (1996).
[3] A. K. Ekert and R. Jozsa, Rev. Mod. Phys. 68, 733 (1996).
[4] http://vesta.physics.ucla.edu/ smolin/index.html
[5] http://www.qubit.org/.
[6]Karen Hunter,SCI 510: Quantum, “Quantum Cryptography”.
[7] Jacob West April 28, 2000.” The Quantum Computer”.
http://www.cs.rice.edu/~taha/teaching/05F/210/news/2005_09_16.htm