ORIGINAL PAPER

THE APROACH OF CLASSICAL COMPUTER TO QUANTUM COMPUTER

SEYEDEH MOHADESEH ELTEJA[1]

Manuscript received: 03.04.2013; Accepted paper: 02.06.2013;

Published online: 15.06.2013.

Abstract. *The aim of this paper is to guide computer scientists through the barriers that separate quantum computing from conventional computing. We introduce basic principles of quantum mechanics to explain where the power of quantum computers comes from and why it is difficult to harness. We describe the diffrences between classical and quantum computers, bit and quantum bit and quantum key distribution.*

Keywords: *classical computer – quantum computer – quantum bit*

1. INTRODUCTION

In 1982 R.Feynman presented an interesting idea how the quantum system can be used for computation reasons. He also gave an explanation how effects of quantum physics could be simulated by such quantum computer. This was very interesting idea which can be used for future research of quantum effects. Every experiment investigating the effects and laws of quantum physics is complicated and expensive. Quantum computer would be a system performing such experiments permanently. Later in 1985, it was proved that a quantum computer would be much more powerful than a classical one.

2. THE DIFFERENCES BETWEEN QUANTUM AND CLASSICAL COMPUTERS

The memory of a classical computer is a string of 0s and 1s, and it can perform calculations on only set of numbers simultaneously. The memory of a quantum computer is a quantum state that can be a superposition of different numbers. A quantum computer can do an arbitrary reversible classical computation on all the numbers simultaneously. Performing a computation on many different numbers at the same time and then interfering all the results to get a single answer, makes a quantum computer much powerful than a classical one. Quantum computer with 500 qubits gives 2^{500}states. Each state would be classically equivalent to a single list of 500 1's and 0's. Such computer could operator on 2^{500}states simultaneously. Eventually, observing the system would cause it to collapse into a single quantum state corresponding to a single answer, a single list of 500 1's and 0's, as dictated by the measurement axiom of quantum mechanics. This kind of computer is equivalent to a classical computer with approximately 10^{150}processors. According to moore's law, the number of transistors of a microprocessor continues to double in every 18 months. According to such evolution if there is a classical computer in year 2020, it will be run at 40 GHZ CPU speed

[1] Shiraz University, Department of Computer Science and Engineering, Shiraz, Iran.
E-mail: mohadeseheltejа@yahoo.com.

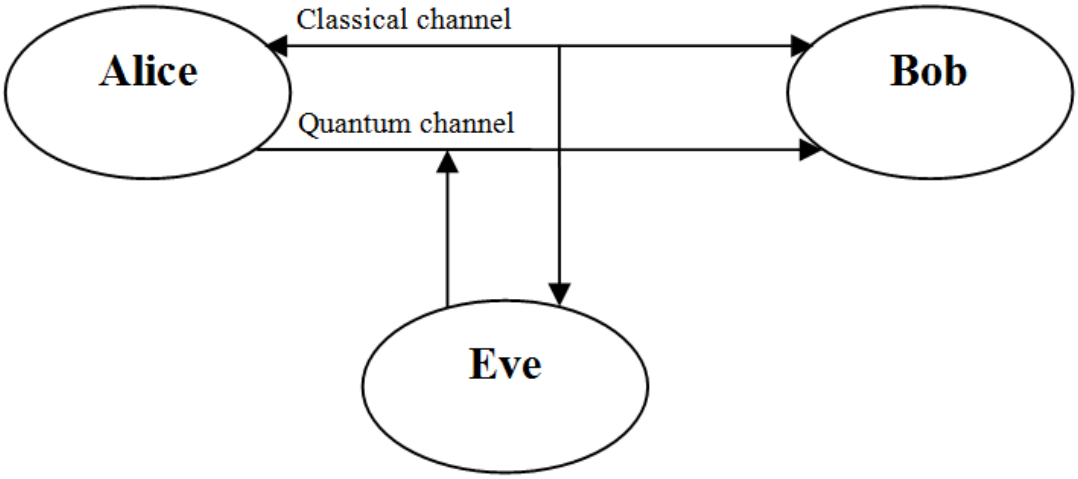
with 160 Gb RAM. If we use an analogue of moor's law for quantum computers, the number of quantum bits would be double in every 18 months. But adding just one qubit is already enough to double a speed. So, the speed of quantum computer will increase more than just doubling it.

3. QUANTUM BITS

A quantum bit, or qubit, is a unit Vector in a two dimensional complex Vector space for which a particular basis, denoted by {10> , |1>}, has been fixed. The orthonormal basis 10> and |1> may correspond to the | ↑> and | → Polarizations of a photon respectively, or to the Polarizations |↗> and | ↖>, or |0 > and |1> could correspond to the spin-up and spin-down states of an electron. When talking about qubits, and quantum computations in general, a fixed basis with respect to which all statements are made has been chosen in advance. In Particular, unless otherwise specified, all measurements will be made with respect to the standard basis for quantum computation, {|0>, |1>}. For the Purposes of quantum computation, the basis states |0> and |1> are taken to represent the classical bit values 0 and 1 respectively. Unlike classical bits however, qubits can be in a superposition of |0> and |1> such as a|0> + b|1>where a and b are complex numbers such that $|a|^2 + |b|^2 = 1$. Just as in the Photon Polarization case, if such a superposition is measured with respect ti the basis {|0> , |1>}, the Probability that the measured value is |0> is $|a|^2$ and the Probability that the measured value is $|b|^2$. Even though a quantum bit can be put in infinitely many superposition states, it is only possible to extract a single classical bit's worth of information from a single quantum bit. The reason that no more information can be gained from a qubit than in a classical bit is that information can only be obtained by measurement. When a qubit is measured, the measurement changes the state to one of the basis states in the way seen in the Photon Polarization experiment. As every measurement can result in only one of two states, one of the basis vectors associated to the given measuring device, so, just as in the classical case, there are only two possible results. As measurement changes the state, one cannot measure the state of a qubit in two different bases.

4. QUANTUM KEY DISTRIBUTION

Sequences of single qubits can be used to transmit private keys on insecure channels. In 1984 Bennett and Brassard described the first quantum key distribution scheme. Classically, public key encryption techniques, e.g.RSA, are used for key distribution. Consider the situation in which Alice and Bob want to agree on secret key so that tjey can communicate privately. They are connected by an ordinary bi-directional open channel and a uni-directional quantum channel both of which can be observed by Eve, who wishes to eavesdrop on their conversation. This situation is illustrated in the figure below. The quantum channel allows Alice to send individual particles (e.g.photons) to Bob who can measure their quantum state. Eve can attempt to measure the state of these particles and can resend the particles to Bob.



To begin the process of estabishing a secret key, Alic sends a sequence of bits to Bob by encoding each bit in the quantum state of a photon as follows. For each bit, Alice randomly uses one of the following two bases for encoding each bit: $0 \rightarrow |\ \rightarrow\!\!\!\!\!\rightarrow, 1 \rightarrow |\ \uparrow\ >$.

Bob measures the state of the Photons he receives by randomly picking either basis. After the bits have been transmitted, Bob and Alice communicate the basis they used for encoding and decoding of each bit over the open channel. With this information both can determine which bits have been transmitted correctly, by identifying those bits for which the sending and receiving bases agree. They will use these bits as the key and discard all the others. On average, Alice and Bob will agree on 50% of all bits transmitted. Suppose the Eve measures the state of the photons transmitted by Alice and resends new photons with the measured state. In this process she will use the wrong basis approximately 50% of the time, in which case she will resend the bit with wrong basis. So when Bob measures a resent qubit with the correct basis there will be a 25% probability that he measures the wrong value. Thus any eavesdropper on the quantum channel is bound to introduce a high error rate that Alice and Bob can detect by communicating a sufficient number of parity bits of their keys over the open channel. So, not only is it likely that Eve's version of the key is 25% incorrect, but the fact that someone is eavesdropping will be apparent to Alice and Bob. Other techniques for enploiting quantum effects for key distribution have been proposed. See for example, Ekert [Ekert at 1992], Bennet [3] and Lo and Chau [4]. Butnone of the quantum key distribution techniques are substitutes for public key encryption schemes. Attacks by eavesdroppers other than the one described here are possible. Security all such schemes are discussed in both Mayers [2] and Loand Chau [4]. Quantum key distribution has been realized over a distance of 24km using standard fiber optical cables [5] and over 0.5 km through the atmosphere [5].

5. CONCLUSIONS

Around 2030 Computers might not have any transistors and chips. Think of a computer that is much faster than a common classical silicon computer. This might be a quantum computer. Theoritically it can run without energy consumption and billion times faster than today's PIII computers. Seientists already think about a quantum computer, as a next generation of classical computers.

REFERENCES

[1] Abrams, D.S., Lloyd, S., *Nonlinear quantum mechanics implies polynomial-time solution for NP-complete and #P problems*, Los Alamos Physics Preprint Archive, 1998. http://xxx.lanl.gov/abs/quant-ph/9801041.

[2] Barenco, A., Bennett, C.H., Cleve, R., Divincenzo, D. P., Margolus, N. H., Shor, P.W., Sleator, T., Smolin, J. A, Weinfurter, H., *Physical Review A* ***52,*** 5, 3457, 1995.

[3] Bennett, C.H., *Physical Review Letters*, **68**(21), 3121, 1992.

[4] Bennett, C. H., Bernstein, E., Brassard, G., Vazirani, U.V., *Society for Industrial and Applied Mathematics Journal on Computing*, **26**(5), 1510, 1997.

[5] Bennett, C.H., Brassard, G., Quantum public key distribution reinvented. *SIGACTN: SIGACT News (ACM Special Interest Group on Automata and Computability Theory)* 18, 1987.

[6] Bennett, C.H., Brassard, G., Ekert, A.K., *Scientific American*, **267**(4), 50, 1992.

[7] Bernstein, E., Vazirani, U.V., Quantum complexity theory. *Society for Industrial and Applied Mathematics Journal on Computing*, **26**(5), 1411, 1997.

[8] Berthiaume, *Quantum computation*. In *Alan L. Selman, Editor, Complexity Theory Retrospective, In Honor of Juris Hartmanis on the Occasion of His Sixtieth Birthday, July 5,* **2**, 1988.

[9] Biron, D., Biham, O., Biham, E., Grassel, M., Lidar, D.A., *Generalized grover search algorithm for arbitrary initial amplitude distribution. Search algorithm for arbitrary initial amplitude distribution*, 1998. Los Alamos Physics Preprint Archive. http://xxx.lanl.gov/abs/quant-ph/9801066