IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661, p- ISSN: 2278-8727Volume 16, Issue 2, Ver. XII (Mar-Apr. 2014), PP 122-125
www.iosrjournals.org

Quantum Computing: Quantum Key Distribution

Vishnu Kumar
(Department of IT, DIT, Dehradun, India)

Abstract : *For the last fifty years computers have grown faster, smaller, and more powerful transforming and benefiting our society in ways too numerous to count. But like any exponential explosion of resources, this growth — known as Moore's law — must soon come to an end. Research has already begun on what comes after our current computing revolution. This research has discovered the possibility for an entirely new type of computer, one that operates according to the laws of quantum physics — a quantum computer.. In this paper, the author will discuss quantum computing and quantum key exchange protocol (BB84) that can be used to securely exchange keys.*

Keywords: *Cryptography, Quantum Computing, Quantum Cryptography, Security*

I. INTRODUCTION

For the last fifty years computers have grown faster, smaller, and more powerful transforming and benefiting our society in ways too numerous to count. But like any exponential explosion of resources, this growth — known as Moore's law — must soon come to an end. Research has already begun on what comes after our current computing revolution. This research has discovered the possibility for an entirely new type of computer, one that operates according to the laws of quantum physics — a quantum computer.

A quantum computer would not just be a traditional computer built out of different parts, but a machine that would exploit the laws of quantum physics to perform certain information processing tasks in a spectacularly more efficient manner. One demonstration of this potential is that quantum computers would break the codes that protect our modern computing infrastructure — the security of every Internet transaction would be broken if a quantum computer were to be built. This potential has made quantum computing a national security concern. Yet at the same time, quantum computers will also revolutionize large parts of science in a more benevolent way. Simulating large quantum systems, something a quantum computer can easily do, is not practically possible on a traditional computer. From detailed simulations of biological molecules which will advance the health sciences, to aiding research into novel materials for harvesting electricity from light, a quantum computer will likely be an essential tool for future progress in chemistry, physics, and engineering. Finally, quantum computers represent a fundamentally new way of approaching information processing and, because this approach is based more closely on how our universe operates, it is likely that building a quantum computer will lead to unforeseen technologies and transform our understanding of the possibilities and limits of computation. For these reasons, as well as increasing international competition in the area, a major national investment should be undertaken in quantum computing and information as part of the new Administration’s science and technology agenda.

A quantum computer (also known as a quantum supercomputer) is a computation device that makes direct use of quantum-mechanical phenomena, such as superposition and entanglement, to perform operations on data. Quantum computers are different from digital computers based on transistors. Whereas 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), quantum computation uses qubits (quantum bits), which can be in superposition of states. A theoretical model is the quantum Turing machine, also known as the universal quantum computer. Quantum computers share theoretical similarities with non-deterministic and probabilistic computers; one example is the ability to be in more than one state simultaneously. The field of quantum computing was first introduced by Yuri Manin in 1980 [1] and Richard Feynman in 1982 [2]. A quantum computer with spins as quantum bits was also formulated for use as a quantum space–time in 1969.

As of 2014 quantum computing is still in its infancy but 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, and many national governments and military funding agencies support quantum computing research to develop quantum computers for both civilian and national security purposes, such as cryptanalysis.

Large-scale quantum computers will be able to solve certain problems much more quickly than any classical computer using the best currently known algorithms, like integer factorization using Shor's algorithm or the simulation of quantum many-body systems. There exist quantum algorithms, such as Simon's algorithm, which run faster than any possible probabilistic classical algorithm [3]. Given sufficient computational resources, however, a classical computer could be made to simulate any quantum algorithm; quantum computation does not violate the Church–Turing thesis.

II. Quantum Key Distribution

Quantum key distribution (QKD) uses quantum mechanics to guarantee secure communication. It enables two parties to produce a shared random secret key known only to them, which can then be used to encrypt and decrypt messages. It is often incorrectly called quantum cryptography, as it is the most well known example of the group of quantum cryptographic tasks.

An important and unique property of quantum distribution is the ability of the two communicating users to detect the presence of any third party trying to gain knowledge of the key. This results from a fundamental aspect of quantum mechanics: the process of measuring a quantum system in general disturbs the system. A third party trying to eavesdrop on the key must in some way measure it, thus introducing detectable anomalies. By using quantum superpositions or quantum entanglement and transmitting information in quantum states, a communication system can be implemented which detects eavesdropping. If the level of eavesdropping is below a certain threshold, a key can be produced that is guaranteed to be secure (i.e. the eavesdropper has no information about it), otherwise no secure key is possible and communication is aborted.

The security of quantum key distribution relies on the foundations of quantum mechanics, in contrast to traditional key distribution protocol which relies on the computational difficulty of certain mathematical functions, and cannot provide any indication of eavesdropping or guarantee of key security.

Quantum key distribution is only used to produce and distribute a key, not to transmit any message data. This key can then be used with any chosen encryption algorithm to encrypt (and decrypt) a message, which can then be transmitted over a standard communication channel. The algorithm most commonly associated with QKD is the one-time pad, as it is provably secure when used with a secret, random key [4].

Quantum communication involves encoding information in quantum states, or qubits, as opposed to classical communication's use of bits. Usually, photons are used for these quantum states. Quantum key distribution exploits certain properties of these quantum states to ensure its security. There are several different approaches to quantum key distribution, but they can be divided into two main categories depending on which property they exploit.

In contrast to classical physics, the act of measurement is an integral part of quantum mechanics. In general, measuring an unknown quantum state changes that state in some way. This is known as quantum indeterminacy, and underlies results such as the Heisenberg uncertainty principle, information-disturbance theorem and no cloning theorem. This can be exploited in order to detect any eavesdropping on communication (which necessarily involves measurement) and, more importantly, to calculate the amount of information that has been intercepted.

The quantum states of two (or more) separate objects can become linked together in such a way that they must be described by a combined quantum state, not as individual objects. This is known as entanglement and means that, for example, performing a measurement on one object affects the other. If an entangled pair of objects is shared between two parties, anyone intercepting either object alters the overall system, revealing the presence of the third party (and the amount of information they have gained).

III. BB84 Key Exchange Protocol

This protocol, known as BB84 after its inventors and year of publication, was originally described using photon polarization states to transmit the information. However, any two pairs of conjugate states can be used for the protocol, and many optical fiber based implementations described as BB84 use phase encoded states. The sender (traditionally referred to as Alice) and the receiver (Bob) are connected by a quantum communication channel which allows quantum states to be transmitted. In the case of photons this channel is generally either an optical fiber or simply free space. In addition they communicate via a public classical channel, for example using broadcast radio or the internet. Neither of these channels need to be secure; the protocol is designed with the assumption that an eavesdropper (referred to as Eve) can interfere in any way with both.

The security of the protocol comes from encoding the information in non-orthogonal states. Quantum indeterminacy means that these states cannot in general be measured without disturbing the original state. BB84 uses two pairs of states, with each pair conjugate to the other pair, and the two states within a pair orthogonal to each other. Pairs of orthogonal states are referred to as a basis. The usual polarization state pairs used are either the rectilinear basis of vertical (0°) and horizontal (90°), the diagonal basis of 45° and 135° or the circular basis of left- and right-handedness. Any two of these bases are conjugate to each other, and so any two can be used in the protocol. Below the rectilinear and diagonal bases are used.

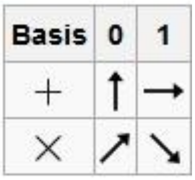
The first step in BB84 is quantum transmission. Alice creates a random bit (0 or 1) and then randomly selects one of her two bases (rectilinear or diagonal in this case) to transmit it in. She then prepares a photon polarization state depending both on the bit value and basis, as shown in the table to the left. So for example a 0 is encoded in the rectilinear basis (+) as a vertical polarization state, and a 1 is encoded in the diagonal basis (x) as a 135° state. Alice then transmits a single photon in the state specified to Bob, using the quantum channel. This process is then repeated from the random bit stage, with Alice recording the state, basis and time of each photon sent. (Refer Figure 1)

According to quantum mechanics (particularly quantum indeterminacy), no possible measurement distinguishes between the 4 different polarization states, as they are not all orthogonal. The only possible measurement is between any two orthogonal states (an orthonormal basis). So, for example, measuring in the rectilinear basis gives a result of horizontal or vertical. If the photon was created as horizontal or vertical (as a rectilinear eigenstate) then this measures the correct state, but if it was created as 45° or 135° (diagonal eigenstates) then the rectilinear measurement instead returns either horizontal or vertical at random. Furthermore, after this measurement the photon is polarized in the state it was measured in (horizontal or vertical), with all information about its initial polarization lost.

As Bob does not know the basis the photons were encoded in, all he can do is to select a basis at random to measure in, either rectilinear or diagonal. He does this for each photon he receives, recording the time, measurement basis used and measurement result. After Bob has measured all the photons, he communicates with Alice over the public classical channel. Alice broadcasts the basis each photon was sent in, and Bob the basis each was measured in. They both discard photon measurements (bits) where Bob used a different basis, which is half on average, leaving half the bits as a shared key.

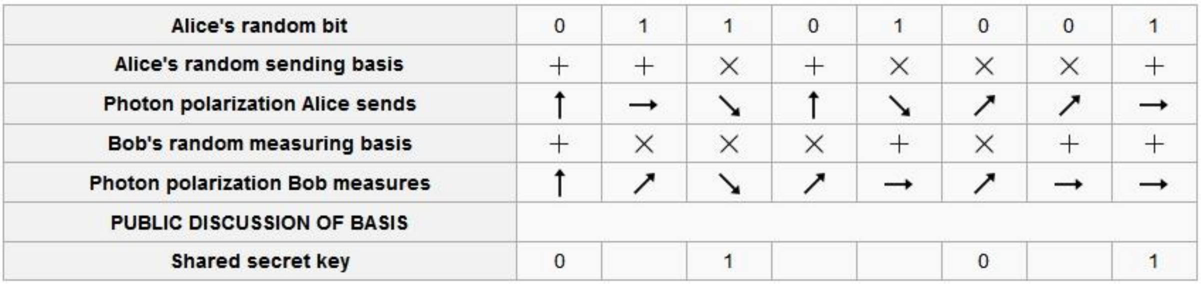
To check for the presence of eavesdropping Alice and Bob now compare a certain subset of their remaining bit strings. If a third party (usually referred to as Eve, for 'eavesdropper') has gained any information about the photons' polarization, this introduces errors in Bob's measurements. If more than p bits differ they abort the key and try again, possibly with a different quantum channel, as the security of the key cannot be guaranteed. p is chosen so that if the number of bits known to Eve is less than this, privacy amplification can be used to reduce Eve's knowledge of the key to an arbitrarily small amount, by reducing the length of the key. (Refer Figure 2)

IV. FIGURES



Basis	0	1
+	↑	→
×	↗	↘

Figure 1 Basis and Polarization



Alice's random bit	0	1	1	0	1	0	0	1
Alice's random sending basis	+	+	×	+	×	×	×	+
Photon polarization Alice sends	↑	→	↘	↑	↘	↗	↗	→
Bob's random measuring basis	+	×	×	×	+	×	+	+
Photon polarization Bob measures	↑	↗	↘	↗	→	↗	→	→
PUBLIC DISCUSSION OF BASIS								
Shared secret key	0		1			0		1

Figure 2 Key Exchange

V. CONCLUSION

Quantum cryptography and especially Quantum Key Distribution (QKD) has triggered intense and prolific research works during the past twenty years and now progresses to maturity. QKD enables Secret Key Establishment between two users, using a combination of a classical channel and a quantum channel, such as an optical fiber link or a free-space optical link. The essential interest of QKD, that is intrinsically linked to the "quantumness" of the signals exchanged on the quantum channel, is that any eavesdropping, on the line can be detected. This property leads to cryptographic properties that cannot be obtained by classical techniques; this property allows performing Key Establishment with an extremely high security standard which is known as unconditional or information-theoretic security. Highly security applications are thus the natural candidates for QKD-based security solutions.

REFERENCES

Journal Papers:

[1] Manin, Yu. I. (1980). *Computable and Noncomputable* (in Russian). Sov.Radio. pp. 13–15. Retrieved 4 March 2013.

[2] Feynman, R. P., *Simulating physics with computers. International Journal of Theoretical Physics* **21** (6): 467–488. Doi: 10.1007/BF02650179.

[3] Simon, D.R. (1994). *"On the power of quantum computation". Foundations of Computer Science, 1994 Proceedings, 35th Annual Symposium on*: 116–123. doi:10.1109/SFCS.1994.365701.

[4] C. H. Bennett, F. Bessette, G. Brassard, L. Salvail and J. Smolin *"Experimental Quantum Cryptography" Journal of Cryptology vol.5*, no.1, 1992, pp. 3-28.