2009 International Symposium on Computing, Communication, and Control (ISCCC 2009)
Proc .of CSIT vol.1 (2011) © (2011) IACSIT Press, Singapore

Modified Quantum Cryptography Using Barcodes

R.P Mahapatra[1], Roopam Mahajan[2] and Rajendra Nahil[3]

[1] Affiliation (Assistant Professor &HOD(CSE), SRM University, NCR Campus, Modi Nagar, U.P. India)
[2] Affiliation ("BTech(CSE) SRM University, NCR Campus, Modi Nagar, U.P. India)
[3] Affiliation ("BTech(CSE),SRM University, NCR Campus, Modi Nagar, U.P. India)

Abstract. Most cryptographic work these days have employed mathematical concept to design cryptosystem and algorithm. Therefore mathematical concept has become critical in designing of cryptosystem and generally used to analyze cryptosystem, most algorithm were based on either factorization or discrete algorithm problem. The system has an overtly simple mathematical background and so requires extensive secondary index computation. Therefore a securer method must be developed to protect system security and to optimize system efficiency. Quantum cryptography detects intrusion and wire trapping. In quantum mechanics a wire trap is not external or passive; but the opposite changing its entity according to the intend component of the system. The system changes once a wire trap is detected.

1. Introduction

Quantum cryptography is an effort to allow two users of a common communication channel to create a body of shared and secret information. This information, which generally takes the form of a random string of bits, can then be used as a conventional secret key for secure communication. It is useful to assume that the communicating parties initially shares a small amount of secret information, which is used up and then renewed in the exchange process, but even without this assumption exchanges are possible.

The advantage of quantum cryptography over traditional key exchange of information can be shown to be secure in a very strong sense without making assumptions about the intractability of certain mathematical problems.

Even when assuming hypothetical eavesdropper with unlimited competency power, the laws of physics guarantee that secret key exchange will be secure, given a few other instructions. When elementary quantum systems such as polarized photon are used to transmit digital information, the uncertainty principle gives rise to the novel cryptographic phenomena.

Unachievable with traditional transmission media.e.g. a communication channel on which it is impossible in principle of eavesdropper without high probability of disturbing the transmission in a such a way as to be detected.

2. Quantum Cryptography

Cryptography greatly relies on the production of random numbers to produce an encryption key- or a string of bits that are used to encode the data and must be known only to the sender and the receiver. Ideally, in order to prevent third parties from being able to decode this key, the string of bits when generated must be as random as possible. Current cryptography systems only generate "quasi random numbers", since they use computer algorithms that can possibly be decoded. Quantum cryptography provides much more security by encoding bits with the quantum properties of photons, which are impossible for third parties to decode. [1]

Cryptographers have tried hard to solve this key distribution problem. The 1970s brought a clever mathematical discovery in the form of public key cryptography (PKC) [6,7]. The idea of PKC is for each

user to randomly choose a pair of mutually inverse transformations -- a scrambling transformation and an unscrambling transformation -- and to publish the directions for performing the former but not the latter. PKC was introduced in 1976[6]

2.1. Cryptography Application

Sending a message using photons is straightforward in principle, since one of their quantum properties, namely polarization, can be used to represent a 0 or a 1. Each photon therefore carries one bit of quantum information, which physicists call a qubit. To receive such a qubit, the recipient must determine the photon's polarization, for example by passing it through a filter, a measurement that inevitably alters the photon's properties. This is bad news for eavesdroppers, since the sender and receiver can easily spot the alterations these measurements cause. Cryptographers cannot exploit this idea to send private messages, but they can determine whether its security was compromised in retrospect. [1]

The genius of quantum cryptography is that it solves the problem of key distribution.[10]

Key distribution problem was written in 1984 by Charles Bennett and Gilles Brassard [11]. In it, Bennett and Brassard described an unconditionally secure quantum key distribution system. The system The first published paper to describe a cryptographic protocol using these ideas to solve the is called the BB84 system (after Bennett and Brassard, 1984), and its operation is as follows [12].

One of the key distribution methods that can be possible is unconditional secure quantum key distribution method.[2]

To eliminate the false measurements from the sequence, Alice and Bob begin a public discussion after the entire sequence of photons has been sent. Bob tells Alice which basis he used to measure each photon, and Alice tells him whether or not it was the correct one. Neither Alice nor Bob announces the actual measurements, only the bases in which they were made. They discard all data for which their polarizers didn't match, leaving (in theory) two perfectly matching strings. They can then convert these into bit strings by agreeing on.

Which photon direction should be 0 or 1?

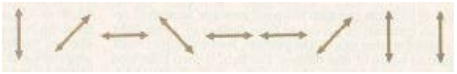
This provides a way for Alice and Bob to arrive at a shared key without publicly announcing any of the bits. If an eavesdropper Eve tries to gain information about the key by intercepting the photons as they are transmitted from Alice to Bob, measuring their polarization, and then resending them so Bob does receive a message, then since Eve, like Bob, has no idea which basis Alice uses to transmit each photon, she too must choose bases at random for her measurements. If she chooses the correct basis, and then sends Bob a photon matching the one she measures, all is well. However, if she chooses the wrong basis, she will then see a photon in one of the two directions she is measuring, and send it to Bob. If Bob's basis matches Alice's (and thus is different from Eve's), he is equally likely to measure either direction for the photon. However, if Eve had not interfered, he would have been guaranteed the same measurement as Alice. In fact, in this intercept/resend scenario, Eve will corrupt 25 percent of the bits. [13]So if Alice and Bob publicly compare some of the bits in their key that should have been correctly measured and find no discrepancies, they can conclude that Eve has learned nothing about the remaining bits, which can be used as the secret key.

2.2. Key Distribution

Quantum cryptography allows two person to transmit there information in the form of secret codes called key.

The key distribution can be expressed if the form of a polarization as illustrated.

Alice sends photon with one of the four polarization state. [1]



For each photon bob chooses random type of measurement: either rectilinear (-) or diagonal(x) type.[1]

Bob records the result of his measurement but keep it a secret [1].

After transmission Bob tell Alice the measurement he used and Alice in return tells about the correct measurement, this process may overhead

Alice and Bob keep all the cases in which the polarization is to measure correctly. After this the cases are converted into 0 and 1 bits.

As a check Alice and Bob chooses sum bit at random to check. If they agree they can use the remaining bit with assurance that they have that they have not been intercepted. [14]

3. Quantum Cryptosystem

Two main channels of communication are used. The first is the quantum channel, the purpose of which is to send and receive quantum bits, and to produce the secret (session) key.

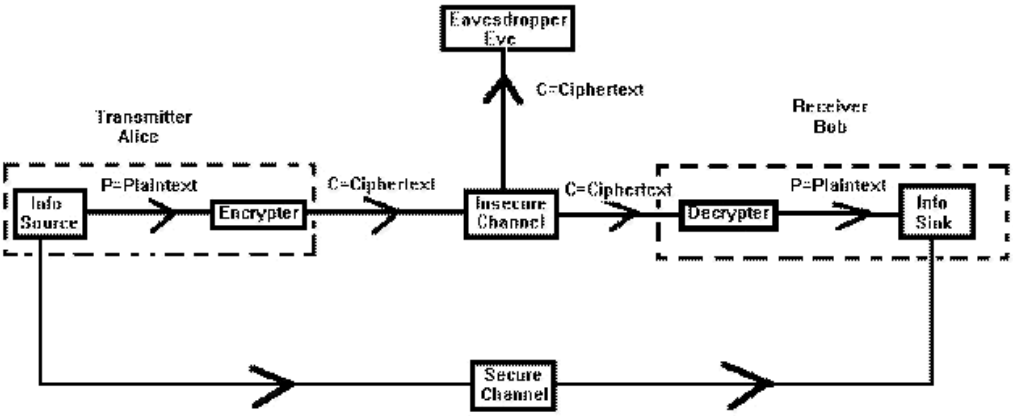


Fig 2: Structure Of Quantum Cryptosystem

Figure 2 shows an analysis of the system structure. The second is the open channel, which is used by the sender and receiver to compare their quantum bits, and thus determine whether they are being tapped; they use their secret (session) key to encrypt plain text and decrypt cipher text, ensuring secure communication.

Once the workings of a quantum crypto system are understood, a quantum cryptographic protocol directed at key distribution can be designed, on the basis that a measurement can affect the quantum status of a system. The protocol is the mechanism for providing security by automatically detecting wire taps.It is not merely the core of the entire system, but also the focus of development. [5]

3.1. Uncertainty Principle

A polarized single photon is used to denote a 0 or 1 bit. Set H is a two-dimensional Hilbert Space whose element represents the polarization of the photon. Two different orthogonal bases, perpendicular polarization and polarization of 45 degrees, within H can be used. [4]

Perpendicular polarization includes Key, such as|↑〉 and |→〉 ; the former represents 1, and the latter 0.Also, 45 degrees polarization includes Key, such as|□〉 and |□〉 ; the former represents 1, and the latter 0.Perpendicular polarization uses the instrument based on the measurement operation symbols, 〈↓|or |→〉 〈←|, to measure the polarization form. In addition, 45 degrees polarization uses the instrument based on measurement operation symbols, |□〉 〈□| or|□〉 〈□| to measure the polarization form. [3]

Instruments used to measure perpendicular polarization cannot be used to measure 45-degree polarization, just as instruments used to measure 45 degrees polarization cannot be used to measure perpendicular polarization.

4. Two Non-Orthogonal Shape Quantum Cryptography

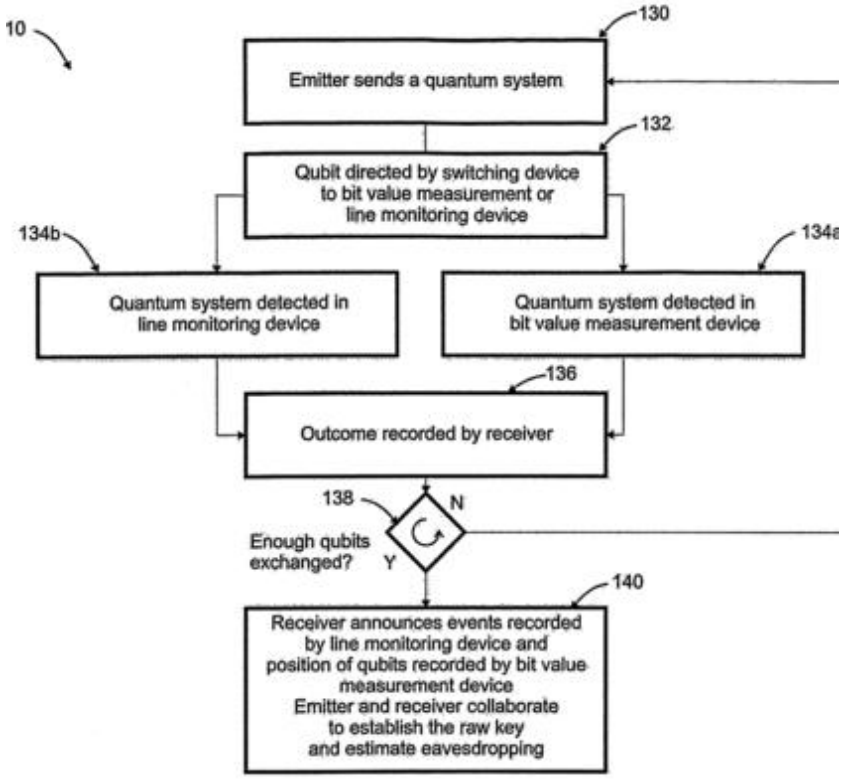


Fig 4: Key Distribution In The Form Of A Flow Chart

An apparatus and method are provided for exchanging between an emitter and a receiver a sequence of bits, also known as the raw key and allowing the emitter and the receiver to estimate the maximum amount of information an eavesdropper can have obtained on the raw key. This raw key can subsequently be distilled into a secure key through an appropriate key distillation procedure [15].

5. Implementation: By Using Bar Codes

A bar code (also barcode) is an optical machine-readable representation of data. Originally, bar codes represented data in the widths (lines) and the spacing of parallel lines and may be referred to as linear or 1D (1 dimensional) barcodes or symbologies. Barcodes can be read by optical scanners called barcode readers or scanned from an image by special software. By using bar codes we can transfer information from one computer to another in a secret manner. [6]

Quantum cryptography is primarily a point-to-point key distribution technique, and when an intermediate piece of networking equipment such as a barcode is introduced into a quantum cryptography path, the operator of the networking equipment can undetectably break the security of the key exchange. [7]

Micro-Electro-Mechanical Systems ("MEMS") comprising mirror arrays can be used to perform optical switching in an optical networking environment. This technology is described in U.S. Pat. No. 5,960,133 to Tomlinson ("Tomlinson"), entitled "Wavelength-Selectable Optical Add-Drop using Tilting Micro-Mirrors." Tomlinson further identifies publications disclosing the necessary technology for fabricating such devices, but Tomlinson fails to suggest the use of such technology in a system for performing quantum cryptographic key exchange. [7]

Consistent with the present invention, methods and systems are provided by which a number of quantum-cryptographic endpoints, such as, for example, computers and firewalls, can be placed into a shared

key distribution network and can exchange QC photons across a network without the network switches being able to read or alter the photons. By using this method information can be transmitted between Alice and Bob in a safe manner.

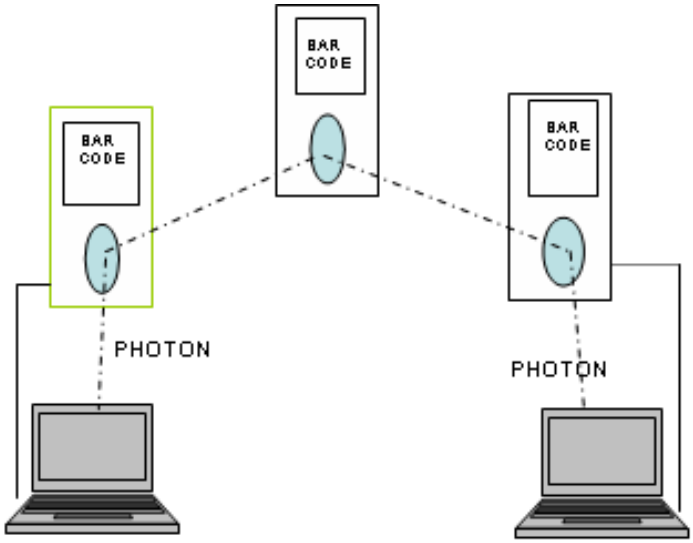


Fig 5: Possible Diagramatic View Using Bar Codes

The above figure shows the block diagram illustration of the key distribution path by using the bar code in between[7].

6. Drawbacks

One of the main drawbacks of quantum cryptography is that, its secured key bit rate is very slow.

a. The problem lies with the fact that some trapped electrons can trigger a delayed echo, which can mislead the device into performing additional detections and corrupting the key. The solution is to temporarily stop the device after the initial detection in order to allow for the electrons to decay. However, this also translates into performance loss and low speed rates [2]

SOLUTION: The solution is to temporarily stop the device after the initial detection in order to allow for the electron to decay. The breakthrough consists of the discovery of a method that allows the detection of much weaker avalanches of electrons. Because the intensity is weaker, the probability of an electron becoming trapped is also significantly reduced, thus no longer requiring stopping the device. This in turn translates into greatly improved transfer rates as well as the possibility for the network to be split in up to 4 nodes. [2]

b. QKD systems developed so far have a vulnerability which leaves them open to hacking. The weak laser diode used to generate single-photon pulses which carry the quantum keys will sometimes generate pulses with multiple photons. [3]

As a result, an eavesdropper could split off and measure one of these extra photons while leaving the other photons in the pulse undisturbed, thus determining part of the key while remaining undetected.

Furthermore, an eavesdropper could determine the entire key by blocking the single-photon pulses and allowing only the multi-photon pulses to travel through the fibre.

SOLUTION: Photon signal pulses are interspersed randomly with a number of "decoy pulses" which can make a pulse splitting attack detectable. The second method, based on nano-technology, features a semiconductor diode that can be controlled with an electrical signal input to emit only single photons at a wavelength compatible with optical fibers. [3]

7. Conclusions

Quantum cryptography promises to revolutionize secure communication by providing security based on the fundamental laws of physics, instead of the current state of mathematical algorithms or computing technology. The devices for implementing such methods exist and the performance of demonstration systems is being continuously improved. Within the next few years, if not months, such systems could start encrypting some of the most valuable technologies.

Other embodiments of the invention will be apparent to those skilled in the art from consideration of the specification and practice of the invention disclosed herein. Principles of quantum mechanics are not limited to any portion of the electromagnetic spectrum. Accordingly, embodiments of the present invention are not constrained to operate only within limits of the human-visible spectrum. Therefore, the terms "light" and "light information", as used and claimed herein, are not necessarily referring to phenomena falling only within the human-visible light spectrum. Moreover quantum principles also apply to physical phenomena other than photons, for example, to entire atoms or their constituent components. Therefore, "light" should be understood in the broad sense of physical waves or particles, rather than its more restricted sense of photons. It is intended that the specification and examples be considered as exemplary only, with a true scope and spirit of the invention being indicated by the following claims.

8. References

[1] http://www.csa.com/discoveryguides/crypt/overview.php has the Brief introduction for quantum cryptography and its classic cryptography. It also tells about the key distribution in the quantum cryptography.

[2] “long distance record ‘quantum keys’ sent 200 kms” News by NATIONAL INSTITUDE OF SCIENCE AND TECHNOLOGY [NIST].

[3] Toshiba article: “Toshiba plug loophole in quantum cryptography

[4] Yu Fang Chung Zhen Yu Wu Feipei Lai1& Tzer Shyong Chen “unconditionally secure cryptosystem based on quantum cryptography” DBLB computer science bibliography.

[5]] Samuel J. Lomonaco, Jr. “Quick glace at quantum cryptography” quant ph-9811056 in 1998.

[6] W. Diffie and M. E. Hellman, IEEE Transactions on Information Theory, IT-22,pp.644-654 (1977).

[7] Rivest R., Shamir A., and Adleman L., "On Digital Signatures and Public-Key Cryptosystems", MIT Laboratory for Computer Science, Technical Report, MIT/LCS/TR-212 (January 1979).

[8] www.virtualschool.edu/mon/ElectronicProperty/klamond/ CCard.htm (K. Lamond, "Credit Card Transactions: Real World and Online”)

[9] E. Klarreich, Nature, vol. 418, 18 July 2002, pp.270-272.

[10] S. K. Moore, IEEE Spectrum, May 2002.

[11] C. H. Bennett and G. Brassard, in Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing, IEEE, New York (1984).

[12] C. H. Bennett, G. Brassard, and A. K. Ekert, "Quantum Cryptography", Scientific American, October 1992, pp. 50-57

[13] C. H. Bennett, "Quantum Cryptography: Uncertainty in the Service of Privacy", Science, vol. 257, 7 August 1992, pp.752-753.

[14] From "Quantum Cryptography" by Charles H. Bennett, Gilles Brassard, and Artur K. Ekert, www.cyberbeach.net/~jdwyer/quantum_crypto/quantum1.htm

[15] From “two non non orthogonal shape quantum cryptography method and apparatus for intra and inter qubic interference” invent by GISIN, Nicolas RIBORDY, Grégoire; ZBINDEN, Hugo.