Authenticated Transmission using Quantum Security

V. Kishore, M. Ramakrishna, M.A.Baseer
Department of Computer Science & Engineering,
SANA Engg. College, JNTUH,
Andhra Pradesh, INDIA.

***Abstract*: Now a day's Security of network transmission became a vital aspect, because the major security risks occur while conducting business on the Net; the following are some of the security risks occur: *Unauthorized-Access, Eavesdropping, Password Sniffing, Denial of Service, Data modification, Repudiation*. One of the methods to secure the information is *Cryptography*. It Protects data transmitted over the network lines, is mainly through appropriate Encryption techniques. The subject Cryptography deals with the encryption and decryption procedures. Encryption is the process of scrambling information so that it becomes unintelligible and can be unscrambled only by using keys. Encryption is the achieved using a *Symmetric* (or) *Asymmetric* Encryption. In Symmetric Encryption, a single key is used encrypt as well as to decrypt. In Asymmetric Encryption, two keys namely public and private key are used for encryption and decryption. The paper presentation is on the Authenticated Transmission using Quantum Security. Quantum cryptography is a new method, which is efficient and fastest of all methods to secure the information. In this Quantum cryptography, main concept is Quantum theory of light, polarization. The foundation of Quantum cryptography lies in the Heisenberg's Uncertainty Principle which states that "*certain pairs of physical properties are related in such a way that measuring one property prevents the observer from simultaneously knowing the value of other*".**

Keywords: Security, Cryptography, Heisenberg's Uncertainty Principle, Quantum cryptography

1. INTRODUCTION

1.1 Introduction to security:

Securely transporting messages has been a goal of all major civilizations. The ancient Greeks, Chinese, and the Spartans are just a few of the ancient civilizations that used some form of cryptography to keep their messages secret [1]. The ciphers used by these civilizations were advanced at the time, but were certainly not unbreakable. Cryptography has evolved over the years to a much more advanced state that our brains alone are incapable of breaking. The most advanced cryptography to date is *Quantum Cryptography*. It was first introduced by Stephen Wiesner in the 1970's.

Quantum cryptography is currently a widely researched topic because of breakthroughs in quantum computing. This makes quantum computing threaten the most widely used key distribution systems used today. Classical cryptography is directly affected by these breakthroughs because it relies solely on the hardness of computing a mathematical problem that are hard be solved by current computers in polynomial time, but theoretically can be solved on a quantum computer. This realization is what provokes the research in quantum cryptography because quantum cryptography does not rely on computational security, but rather on the laws of quantum physics. This paper will first give a brief history of classical cryptography and discuss its different kinds. Then quantum cryptography and the most famous quantum key distribution protocol are taken into account along with a description of what eavesdropping is and how quantum cryptography defends against it.

1.2 Introduction to cryptography:

Cryptography is one of the host authentication technique used in making a network channel secure to transmit confidential data. In cryptographic system, the original intelligible message is known as plaintext is converted in to random nonsense known as ciphertext. This cipher is transmitted at the receiver end; the random nonsense is converted back to the plaintext.

In cryptographic system, the algorithm that is used for Encryption the plaintext to ciphertext, decrypting the cipher text to plaintext is kept open, the key that are used for encryption and decryption must be maintained secretly.

Eavesdropping is the act of an unintended receiver intercepting and reading a message between two communicating parties. Preventing eavesdropping is one of the main priorities of any key distribution system and quantum key distribution systems have an advantage. Quantum theory has a principle called the Heisenberg uncertainty principle that guarantees any effort to monitor the communication will disturb it in some detectable way. Although this does not prevent eavesdropping, it will allow the communicating parties to know if someone is eavesdropping. If someone is detected eavesdropping, the communicating parties can disregard the current key and not lose anything significant since it was a randomly generated key [7].

1.3 Introduction to Quantum cryptography:

Quantum cryptography uses our current knowledge of physics to develop a cryptosystem that is not able to be defeated - that is, one that is completely secure against being compromised without knowledge of the sender or the receiver of the messages. The word quantum itself refers to the most fundamental behavior of the smallest particles of matter and energy: quantum theory explains everything that exists and nothing can be in violation of it.

Quantum cryptography is different from traditional cryptographic systems in that it relies more on physics, rather than mathematics, as a key aspect of its security model.

Essentially, quantum cryptography is based on the usage of individual particles/waves of light (photon) and their intrinsic quantum properties to develop an unbreakable cryptosystem - essentially because it is impossible to measure the quantum state of any system without disturbing that system. It is theoretically possible that other particles could be used, but photons offer all the necessary qualities needed, their behavior is comparatively well-understood, and they are the information carriers in optical fiber cables, the most promising medium for extremely high-bandwidth communications.

2. TYPES OF CRYPTOGRAPHY

2.1 Classical Cryptography:

Cryptography is the art of devising *codes* and *ciphers* and C***ryptanalysis*** is the art of breaking them. ***Cryptology*** is the combination of these two. In the literature of cryptology, information to be encrypted is known as *plaintext*, and the parameters of the encryption algorithm that transforms the plaintext are collectively called a *key*. The keys used to encrypt most messages before being sent, such as credit-card information exchange over the Internet. The schemes used to disguise keys are thought to be secure, because discovering them would take too long for even the fastest computers.

Existing cryptographic techniques are usually identified as "traditional" and "modern." Traditional techniques date back for centuries, and use operations of coding, transposition, and substitution. Traditional techniques were designed to be simple, for hand encoding and decoding. By contrast, modern techniques use computers, and rely on extremely long keys, convoluted algorithms, and intractable problems to achieve assurances of security.

There are two branches of modern cryptographic techniques: *Symmetric key* encryption and *Asymmetric key(PKC)* encryption. In PKC, messages are exchanged using an encryption method so convoluted that even full disclosure of the scrambling operation provides no useful information for how it can be undone. Each participant has a pair of "public key" and a "private key", the former is used by others to encrypt messages, and the latter is used by the participant to decrypt them. The widely used RSA algorithm is one example of PKC.

Anyone wanting to receive a message publishes a key, which contains two numbers. A sender converts a message into a series of digits, and performs a simple mathematical calculation on the series using the publicly available numbers. Messages are deciphered by the recipient by performing another operation, known only to him. In principle, an eavesdropper could deduce the decryption method by factoring one of the published numbers, but this is chosen to typically exceed 300 digits and to be the product of only two large *prime numbers*, so that there is no known way to accomplish this factorization in a practical time.

In secret key encryption, a *k*-bit "secret key" is shared by two users, who use it to transform plaintext inputs to crypto text for transmission and back to plaintext upon receipt. To make unauthorized decipherment more difficult, the transformation algorithm can be carefully designed to make each bit of output depend on every bit of the input. With such an arrangement, a key of 128 bits used for encoding results in a choice of about 10^{38} numbers. The encrypted message should be secure; assuming that brute force and massive parallelism are employed; a billion computers doing a billion operations per second would require a trillion years to decrypt it. In practice, analysis of the encryption algorithm might make it more vulnerable, but increases in the size of the key can be used to offset this.

The main practical problem with secret key encryption is exchanging a secret key. In principle any two users who wished to communicate could first meet to agree on a key in advance, but in practice this could be inconvenient. Other methods for establishing a key, such as the use of secure courier or private knowledge, could be impractical for routine communication between many users. But any discussion of how the key is to be chosen that takes place on a public communication channel could in principle be intercepted and used by an eavesdropper.

One proposed method for solving this is the appointment of a central key distribution server. Every potential communicating party registers with the server and establishes a secret key. The server then relays secure communications between users, but the server itself is vulnerable to attack. Another method is a protocol for agreeing on a secret key based on publicly exchanged large prime numbers, as in the Diffie Hellman key exchange. Its security is based on the assumed difficulty of finding the power of a base that will generate a specified remainder when divided by a very large prime number, but this suffers from the uncertainty that such problems will remain intractable. Quantum encryption provides a way of agreeing on a secret key without making this assumption.

Communication at the quantum level is far more different from both classical secret key and public key communication. For example, it is not necessarily possible for messages to be perfectly copied by anyone with access to them, nor for messages to be relayed without changing them in some respect, nor for an eavesdropper to passively monitor communications without being detected.

2.2 Quantum Cryptography:

The foundation of quantum cryptography lies in the Heisenberg uncertainty principle, which states that certain pairs of physical properties are related in such a way that measuring one property prevents the observer from simultaneously knowing the value of the other. In particular, when measuring the polarization of a photon, the choice of what direction to measure affects all subsequent measurements. For instance, if one measures the polarization of a photon by noting that it passes through a vertically oriented filter, the photon emerges as vertically polarized regardless of its initial direction of polarization.

Quantum cryptography provides means for two parties to exchange an enciphering key over a private channel with compielt security of communication. There are at least three main types of quantum cryptosystems for the key distribution.

(a) Cryptosystem with encoding based on two non-commuting observable.
(b) Cryptosystem with encoding based on two non-orthogonal state vectors.
(c) Cryptosystems with encoding built upon quantum entanglement and the bell theorem.

The basic idea of cryptosystems is a sequence of correlated particle pairs is generated, with one member of each pair being detected by each party. An eavesdropper on this communication would have to detect a particle to read the signal, and retransmit it in order for his presence to remain unknown. However, the act of detection of one particle of a pair destroys its quantum correlation with the other, and the two parties can easily verify whether this has been done, without revealing the results of their own measurements, by communication over an open channel.

3. History of Quantum Cryptography

The roots of quantum cryptography are in a proposal by Stephen Weisner called “Conjugate Coding” from the early 1970s. It was eventually published in 1983 in Sigact News, and by that time Bennett and Brassard, who were familiar with Weisner's ideas, were ready to publish ideas of their own. They produced “BB84”" the first quantum cryptography protocol, in 1984, but it was not until 1991 that the first experimental prototype based on this protocol was made operable (over a distance of 32 centimeters). More recent systems have been tested successfully on fiber optic cable over distances in the kilometers.

Several years before the discovery of public-key cryptography, another striking development had quietly taken place: the union of cryptography with quantum mechanics. Around 1970 Stephen J. Wiesner, then at Columbia University, wrote a paper entitled "Conjugate Coding," explaining how quantum physics could be used, at least in principle, to accomplish two tasks that were impossible from the perspective of classical physics. One task was a way to produce bank notes that would be physically impossible to counterfeit. The other was a scheme for combining two classical messages into a single quantum transmission from which the receiver could extract either message but not both. Unfortunately, Wiesner's paper was rejected by the journal to which he sent it, and it went unpublished until 1983. Meanwhile, in 1979, two of us (Bennett and Brassard) who knew of Wiesner's ideas began thinking of how to combine them with public-key cryptography.

We soon realized that they could be used as a substitute for PKC: two users, who shared no secret initially, could communicate secretly, but now with absolute and provable security, barring violations of accepted physical laws.

4. Working of Quantum Key Distribution

The most straightforward application of quantum cryptography is in distribution of secret keys. The amount of information that can be transmitted is not very large, but it is provably very secure. By taking advantage of existing secret-key cryptographic algorithms, this initial transfer can be leveraged to achieve a secure transmission of large amounts of data at much higher speeds. Quantum cryptography is thus an excellent replacement for the Diffie-Hellman key exchange algorithm.

How It Works in Theory

In theory, quantum cryptography works in the following manner: Assume that two people wish to exchange a message securely, traditionally named Alice and Bob. Alice initiates the message by sending Bob a key, which will be the mode for encrypting the message data. This is a random sequence of bits, sent using a certain type of scheme, which can see two different initial values represent one particular binary value (0 or 1).

Let us assume that this key is a stream of photons travelling in one direction, with each of these photon particles representing a single bit of data (either a 0 or 1). However, in addition to their linear travel, all of these photons are oscillating (vibrating) in a certain manner. These oscillations can occur in any 360-degree range across any conceivable axis, but for the purpose of simplicity (at least as far as it is possible to simplify things in quantum cryptography), let us assume that their oscillations can be grouped into 4 particular states: we'll define these as UP/DOWN, LEFT/RIGHT, UPLEFT/RIGHTDOWN and UPRIGHT/LEFTDOWN. The angle of this vibration is known as the polarization of the photon. Now, let us introduce a polarizer into the equation. A polarizer is simply a filter that permits certain photons to pass through it with the same oscillation as before and lets others pass through in a changed state of oscillation (it can also block some photons completely, but let's ignore that property for this exercise). Alice has a polarizer that can transmit the photons in any one of the four states mentioned - in effect, she can choose either rectilinear (UP/DOWN and LEFT/RIGHT) or diagonal (UPLEFT/RIGHTDOWN and UPRIGHT/ LEFTDOWN) polarization filters.

Alice swaps her polarization scheme between rectilinear and diagonal filters for the transmission of each single photon bit in a random manner. In doing so, the transmission can have one of two polarizations represent a single bit, either 1 or 0, in either scheme she uses.

When receiving the photon key, Bob must choose to measure each photon bit using either his rectilinear or diagonal polarizer: sometimes he will choose the correct polarizer and at other times he will choose the wrong one. Like Alice, he selects each polarizer in a random manner. So what happens with the photons when the wrong polarizer is chosen?

The Heisenberg Uncertainty Principle states that we do not know exactly what will happen to each individual photon, for in the act of measuring its behavior, we alter its properties (in addition to the fact that if there are two properties of a system that we wish to measure, measuring one precludes us from quantifying the other). However, we can make a guess as to what happens with them as a group. Suppose Bob uses a rectilinear polarizer to measure UPLEFT/RIGHTDOWN and UPRIGHT/LEFTDOWN (diagonal) photons. If he does this, then the photons will pass through in a changed state - that is, half will be transformed to UP/DOWN and the other half to LEFT/RIGHT. But we cannot know which individual photons will be transformed into which state (it is also a reality that some photons may be blocked from passing altogether in a real world application, but this is not relevant to the theory).

Bob measures some photons correctly and others incorrectly. At this point, Alice and Bob establish a channel of communication that can be insecure - that is, other people can listen in. Alice then proceeds to advise Bob as to which polarizer she used to send each photon bit - but not how she polarized each photon. So she could say that photon number 8597 (theoretically) was sent using the rectilinear scheme, but she will not say whether she sent an UP/DOWN or LEFT/RIGHT. Bob then confirms if he used the correct polarizer to receive each particular photon. Alice and Bob then discard all the photon measurements that he used the wrong polarizer to check. What they have, is, on average, a sequence of 0s and 1s that is half the length of the original transmission...but it will form the basis for a one-time pad, the only cryptosystem that, if properly implemented, is proven to be completely random and secure.

Now, suppose we have an eavesdropper, Eve, who attempts to listen in, has the same polarizer's that Bob does and must also randomly choose whether to use the rectilinear or diagonal one for each photon. However, she also faces the same problem that Bob does, in that half the time she will choose the wrong polarizer. But Bob has the advantage of speaking to Alice to confirm which polarizer type was used for each photon. This is useless to Eve, as half the time she used the wrong detector and will misinterpret some of the photons that will form that final key, rendering it useless.

Furthermore, there is another level of security inherent in quantum cryptography - that of intrusion detection. Alice and Bob would know if Eve was eavesdropping on them. The fact that Eve is on the "photon highway" can become obvious because of the following.

Let's say that Alice transmits photon number 349 as an UPRIGHT/LEFTDOWN to Bob, but for that one, Eve uses the rectilinear polarizer, which can only measure UP/DOWN or LEFT/RIGHT photons accurately. What Eve will do is transform that photon into either UP/DOWN or LEFT/RIGHT, as that is the only way the photon can pass. If Bob uses his rectilinear polarizer, then it will not matter what he measures as the polarizer check Alice and Bob go through above will discard that photon from the final key. But if he uses the diagonal polarizer, a problem arises when he measures its polarization; he may measure it correctly as UPRIGHT/LEFTDOWN, but he stands an equal chance, according to the Heisenberg Uncertainty Principle, of measuring it incorrectly as UPLEFT/RIGHTDOWN. Eve's use of the wrong polarizer will warp that photon and will cause Bob to make errors even when he is using the correct polarizer.

To discover Eve's nefarious doings, they must perform the above procedures, with which they will arrive at an identical key sequence of 0s and 1s - unless someone has been eavesdropping, whereupon there will be some discrepancies. They must then undertake further measures to check the validity of their key. It would be foolish to compare all the binary digits of the final key over the unsecured channel discussed above, and also unnecessary.

Let us assume that the final key comprises 4,000 binary digits. What needs to be done is that a subset of these digits be selected randomly by Alice and Bob, say 200 digits, in terms of both position (that is, digit sequence number 2, 34, 65, 911 etc) and digit state (0 or 1). Alice and Bob compare these - if they match, then there is virtually no chance that Eve was listening. However, if she was listening in, then her chances of being undiscovered are one in countless trillions, that is, no chance in the real world. Alice and Bob would know someone was listening in and then would not use the key - they would need to start the key exchange again over a secure channel inaccessible to Eve, even though the comparisons between Alice and Bob discussed above can still be done over an insecure channel. However, even if Alice and Bob have concluded that the their key is secure, since they have communicated 200 digits over an un-secure channel, these 200 digits should be discarded from the final key, turning it from a 4,000 into a 3,800 bit key).

Thus, quantum cryptography is a way to combine the relative ease and convenience of key exchange in public key cryptography with the ultimate security of a onetime pad.

How It Works in Practice

In practice, quantum cryptography has been demonstrated in the laboratory by IBM and others, but over relatively short distances. Recently, over longer distances, fiber optic cables with incredibly pure optic properties have successfully transmitted photon bits up to 60 kilometers. Beyond that, BERs (bit error rates) caused by a combination of the Heisenberg Uncertainty Principle and microscopic impurities in the fiber make the system unworkable. Some research has seen successful transmission through the air, but this has been over short distances in ideal weather conditions. It remains to be seen how much further technology can push forward the distances at which quantum cryptography is practical.

Practical applications in the US are suspected to include a dedicated line between the White House and Pentagon in Washington, and some links between key military sites and major defense contractors and research laboratories in close proximity.

5. AN EXAMPLE PROTOCOL

This section describes the general protocol for agreeing on a secret key, as described by Bennett et al. [1991]. It uses polarization of photons as its units of information. Polarization can be measured using three different bases, which are conjugates: rectilinear (horizontal or vertical), circular (left-circular or right-circular), and diagonal (45 or 135 degrees). Only the rectilinear and circular bases are used in the protocol, but the diagonal basis is slightly useful for eavesdropping.

1. A polarized beam in short bursts with a very low intensity. The polarization in the light source, often a light-emitting diode (LED) or laser, is filtered to produce each burst is then modulated randomly to one of four states (horizontal, vertical, left-circular, or right-circular) by the sender, Alice.
2. The receiver, Bob, measures photon polarizations in a random sequence of bases (rectilinear or circular).
3. Bob tells the sender publicly what sequences of bases were used.
4. Alice tells the receiver publicly which bases were correctly chosen.
5. Alice and Bob discard all observations not from these correctly chosen bases.
6. The observations are interpreted using a binary scheme: left circular or horizontal is 0, and right circular or vertical is 1.

This protocol is complicated by the presence of noise, which may occur randomly or may be introduced by eavesdropping. When noise exists, polarizations observed by the receiver may not correspond to those emitted by the sender. In order to deal with this possibility, Alice and Bob must ensure that they possess the same string of bits, removing any discrepancies. This is generally done using a binary search with parity checks to isolate differences; by discarding the last bit with each check, the public discussion of the parity is rendered harmless. In the Bennett et al. [1991] protocol, this process is

1. The sender, Alice, and the receiver, Bob, agree on a random permutation of bit positions in their strings (to randomize the location of errors).
2. The strings are partitioned into blocks of size *k* (*k* ideally chosen so that the probability of multiple errors per block is small).
3. For each block, Alice and Bob compute and publicly announce parities. The last bit of each block is then discarded.
4. For each block for which their calculated parities are different, Alice and Bob use a binary search with log (*k*) iterations to locate and correct the error in the block.
5. To account for multiple errors that might remain undetected, steps 1-4 are repeated with increasing block sizes in an attempt to eliminate these errors.
6. To determine whether additional errors remain, Alice and Bob repeat a randomized check:
   - Alice and Bob agree publicly on a random assortment of half the bit positions in their bit strings.
   - Alice and Bob publicly compare parities (and discard a bit). If the strings differ, the parities will disagree with probability 1/2.
   - If there is disagreement, Alice and Bob use a binary search to find and eliminate it, as above.
7. If there is no disagreement after *l* iterations, Alice and Bob conclude their strings agree with low probability of error (2^{-l}).

6. Quantum Cryptography Applications

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.

The genius of quantum cryptography is that it solves the problem of key distribution. A user can suggest a key by sending a series of photons with random polarizations. This sequence can then be used to generate a sequence of numbers. The process is known as quantum key distribution. If the key is intercepted by an eavesdropper, this can be detected and it is of no consequence, since it is only a set of random bits and can be discarded. The sender can then transmit another key. Once a key has been securely received, it can be used to encrypt a message that can be transmitted by conventional means: telephone, e-mail, or regular postal mail.

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

The BB84 system is now one of several types of quantum cryptosystems for key distribution. Another one involves cryptosystems with encoding built upon quantum entanglement and Bell's Theorem, proposed by Artur K. Ekert (1990). The basic idea of those cryptosystems is as follows. A sequence of correlated particle pairs is generated, with one member of each pair being detected by each party. An eavesdropper on this communication would have to detect a particle to read the signal, and retransmit it in order for his presence to remain unknown. However, the act of detection of one particle of a pair destroys its quantum correlation with the other, and the two parties can easily verify whether this has been done, without revealing the results of their own measurements, by communication over an open channel.

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 secrets of government and industry.

The genius of quantum cryptography is that it solves the problem of key distribution. The advantage of quantum cryptography over traditional key exchange methods is that the 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 eavesdroppers with unlimited computing power, the laws of physics guarantee (probabilistically) that the secret key exchange will be secure, given a few other assumptions.

References:

[1] Kartalopoulos, S.V. 2006, "A primer on cryptography in communications", IEEE Communications Magazine, 44, (4), 146 - 151.

[2] Network Security Essentials – William Stallings.

[3] Cryptography and Network Security – William Stallings.

[4] Applied Cryptography – Schneider

[5] Handbook of applied Cryptography – Menezes, Vanstone, Van Oorshot

[6] Report on the development of the advanced encryption Standard – NIST'S adhoc AES selection team

[7] Bennett, C. H.1992, "Quantum cryptography using any two non orthogonal states", Physical Review Letters, 68, (21), 3121–3124.

[8] Bennett C H, Brassard G, Cr´epeau C and Maurer U M 1995 *IEEE Trans. Inform. Theory* **41** 1915