IJESRT
INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

Enhancement of Quantum Key Distribution Protocol.

Chainika Singhal [*1], Ravinder Kr.Gautam [2], Lakshman Das[3], Manoj Kumar.Mishra[4]
[*1,4] VIET, Ghaziabad
[2,3] HIET, Ghaziabad
chainikasinghal@gmail.com

Abstract

Primarily, we know Quantum cryptographic technique replaces classical cryptography and give a review on the first QKD protocol which secrecy is guaranteed by physics of Quantum mechanics through which the problem of secure key transmission of classical cryptography solved. But we find that there are many vulnerabilities in existing model of Quantum key distribution protocol and this paper represents the proposed model of Quantum key distribution protocol.

Keyword: Quantum Key, Cryptography

Quantum Cryptography

Describes the use of Quantum mechanical effects (in particular quantum communication and Quantum computation) to perform cryptographic tasks or to break cryptographic systems.

Quantum Key Distribution (QKD)

Allows two parties to communicate in absolute privacy during the presence of an eavesdropper, i.e. passive listener. The Heisenberg uncertainty principle of quantum mechanics assures a detection of the presence of an eavesdropper located somewhere on a quantum channel. In addition, an eavesdropper can't copy unknown qubits i.e. unknown quantum states, due to no-cloning theorem which was first shown by Wooters and Zurek in 1984 [1].

As we know Quantum cryptographic technique replaces classical cryptography and give a review on the first QKD protocol which secreacy is guaranteed by physics of Quantum mechanics.

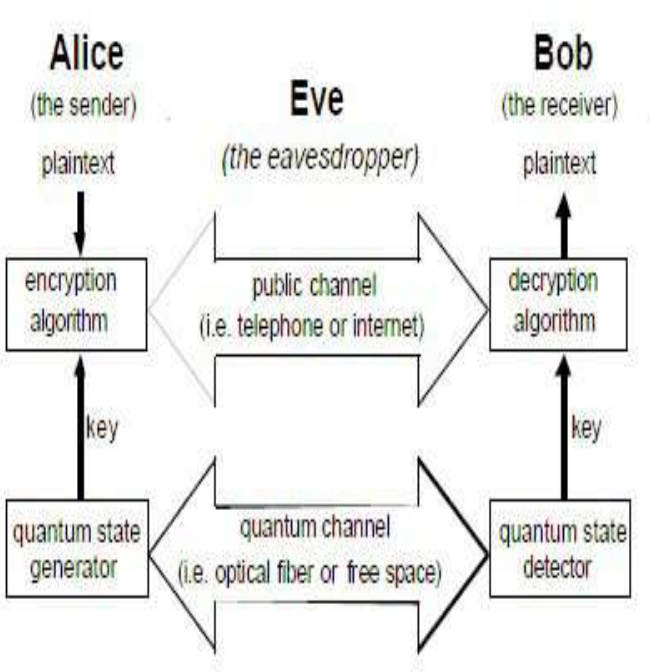
Problem In Classical Cryptography

The major problem in classical cryptography is key distribution . If Alice and Bob want to communicate securely, they need to share a secret key before any encryption process can be started. Except, not so practical solution like the face-to-face meeting, there exist two main solutions: asymmetrical (public key) cryptosystems and quantum cryptography.

In public-key cryptosystems, each person has a private and a public key. If Alice wants to send a plaintext (a secret key) to Bob, she will encrypt the plaintext with Bob's public key. Bob will then decrypt the cryptogram with his private key. Public-key cryptosystem was first proposed in 1976 by Whitfield Diffie and Martin Hellman. The first implementation was then developed by Ronald Rivest, Adi Shamir, and Leonard Adleman in 1978. The problem is that Security and future use of these systems depends on further theoretical and mathematical progress. Some mathematical problems, like prime factorization and discrete logarithm calculation, are foundations of the most widely used public-key cryptosystems today. Theoretical results from last decade showed that quantum mechanical principles can be used to extract more computational power than any classical information processing can do. The progress of present technology can't follow fast progress of theory, but some parts of quantum information processing were experimentally shown. Mainly, that experimental progress is related to the quantum cryptography – quantum key distribution (QKD). For more information on quantum information and computation see [2,3,4].

The second solution on the key distribution problem is QKD. QKD is the way of generating a secret key to both parties in a process of repetitive communication. During the QKD, Alice and Bob use two channels: a classical public channel and a quantum channel. First, Alice sends quantum bits, i.e. qubits or photons to Bob over the quantum channel which could be an optical fiber or a free-space optical link. Bob is measuring those qubits obtaining so a sequence of bits. The sequence depends on a coding ystem between two parties and chosen measurements which have random characteristics. Then Alice and Bob communicate over the public channel, in order to agree or disagree with Bob's received bits. This

procedure must be repeated few times in order to make some error corrections and to gather enough bits



to form a secret key.

Fig.1 : A Quantum Cryptographic communication system for securely transferring random key

Quantum Key Exchange

A central problem in cryptography is the key distribution problem. One solution is based on mathematics, public key cryptography. Another approach is based on physics: quantum cryptography. While Public Key Cryptography relies on computational difficulty of certain hard mathematical Problems (such as integer factorization).Quantum cryptography relies on the laws of quantum mechanics.

Quantum cryptographic devices typically imply individual photons of light and take advantage of either the Heisenberg Uncertainty Principle or Quantum entanglement.

Uncertainty

The act of measurement is an integral part of Quantum mechanics not just a passive external process as in classical physics. So, it is possible to encode information into some quantum properties of a photon in such a way that any effort to monitor them necessarily disturb them in some detectable way, the effect arises because in the quantum theory certain pairs of physical properties are complementary in the sense that measuring one property necessarily disturbs the other. This statement is known as Heisenberg Uncertainty Principle. It doesn't refer merely to the limitation of a particular measurement technology: it holds for all possible measurements. The two complementary properties that are often used in the quantum cryptography are the two type of photons polarization e.g. rectilinear (vertical and horizontal) and diagonal(at 45ºand 135º**).**

Enhancement

It is a state of two or more quantum particles e.g. photons in which many of their physical properties are strongly correlated . The entangled can't be described by specify the states of individual particles and they meet together shared information in a form which can't be accessed in any experiment performed on either of the particles alone. This happens no matter how far apart the particles may be at the time is crucial for long distance quantum key distribution.

TWO Different Approaches

Based on these two counter intuitive features of quantum mechanics (uncertainty and entanglement), two different types of quantum cryptographic protocols were invented. Both are based on the fact that quantum systems are disturbed by measurements performing on them. The first type uses of polarization of photon to encode the bits of information in rely on quantum randomness to keep Eve from learning the secret key. e.g BB84 & B92 Protocols. The second type of entangled photon relies on the fact that the information defining the key only "comes into being" after measurement per Alice & Bob e.g. EPR protocol**.**

Review of Existing Quantum Key Distribution Protocol Model

A lot of quantum key distribution protocols have been put forward nowadays, which can be divided into two kinds one is based upon non-orthogonal or non-exchange quantum form, another is based upon quantum-tangle. In the factual telecommunication system, all the quantum key distribution protocols need four processes as Fig 2.

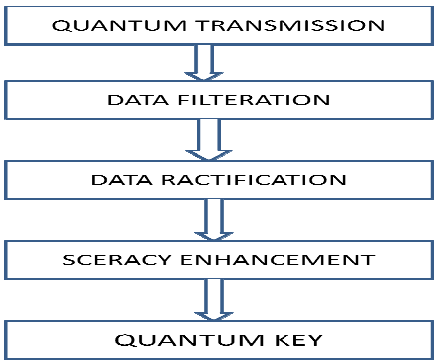


Figure 2 . Original quantum key distribution chart

Vulnerability In Existing Model

- **No authentication of participant**

In existing QKD protocol model we do not check the identity of communicating party that leads the probability of sharing secret key with unknown person. This unknown person may be attacker or can misuse the key. Another thread of no authentication is man in middle attack.

- **Lack of pre transmission process**

Before quantum transmitting the participant of key distribution (let Alice and Bob) require some pre process to ensure that is Alice/ bob is ready to send/receive the transmission respectively? If we do not do preprocess that leads to wastage of time & wastage of resource. This also increase the error rate in QKD that increase probability of Inaccurate key generation

- **No estimation of attackers information**

As we know QKD is secure by No cloning theorem & Heisenberg uncertainty principle..But attacker always tries new methods to get information. Attacker is present in two mode either Active mode or Passive mode ,so our protocol should strong enough to detect presence of attacker & to estimating the amount of information that attacker can get.

The Proposed Model of Quantum Key Distribution Protocol With Improvement

The improvement of quantum key distribution is realize nine steps that are:

1. Authentication of participant in QKD,
2. Initialization,
3. Quantum Transmission,
4. Shifting,
5. Error Correction,
6. Estimating Attacker's Information,
7. Decision on continuation,
8. Privacy amplification,
9. Getting error free key.

The relationship between the steps is displayed in Fig.3.

In the improvement, a conservative assumption is that all the errors are made by the attacker, which can enhance the protocol security greatly. Meanwhile system wastage is ignored

1. Authentication of participant

It is very important to check the authenticity of participant in the beginning. Authentication of participant adopts the method referred in reference [6]. For authentication we use both classical and quantum channel. For future we can also use particular photon polarization for authentication. [8]

2. Initialization

Is Bob ready to receive the transmission send by Alice or is Alice ready to send transmission. If one of them is not ready then it is wastage of time so we need checking Process

"Initialization"= "checking" + "prepare to ready".

For Initialization request information and reply information can exchanged by public channel between the sender Alice and the receiver Bob. Alice and Bob adopt a pre-define protocol to convert the polarization to bits. But for ultimate security at beginning we propose that "Quantum handshake protocol" is used for initialization.[9]

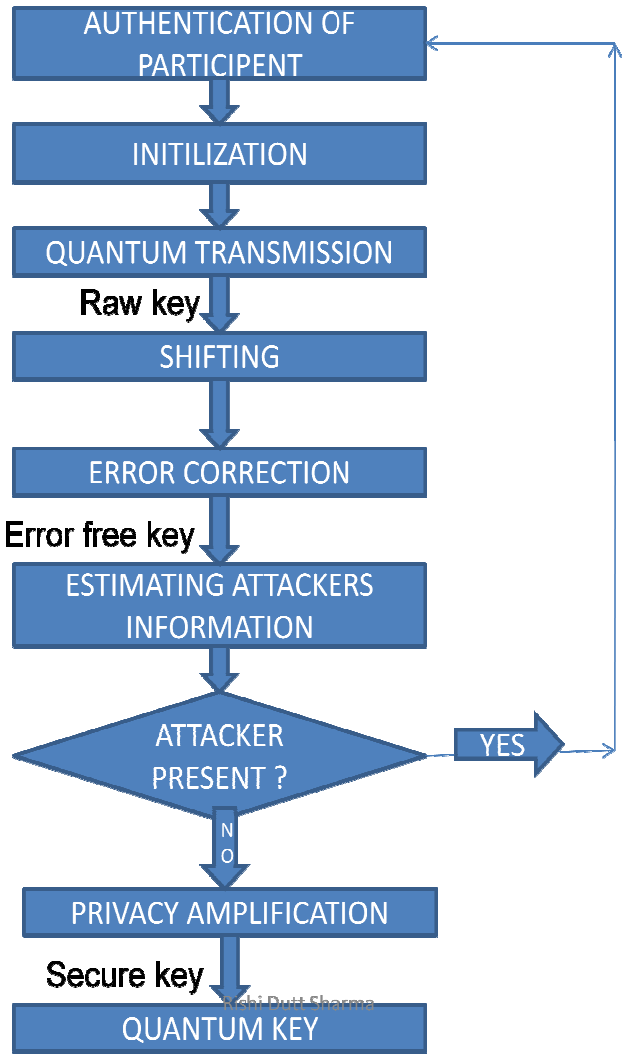


Figure3. A proposed flowchart of the basic quantum key distribution protocol

3. Quantum transmission

From here actual transmission is start .Quantum transmission adopts single- quantum channel method that is "Raw Quantum Transmission , RQT". Photon gun is used to generate photon.

Alice send raw key to Bob.

4. Shifting

In the sifting step, Alice and Bob use a public channel to communicate information related to their measurement, in particular what basis they used to prepare or measure their qubits and at what times

Channel	Bit Error Rate(%)
0°	1.32
45°	2.54
90°	2.20
135°	4.75

they registered a detection event. They do not disclose the measurement result whenever Alice and Bob used the same basis, they should get perfectly correlated bits. The process of discarding the bits in the cases where they used different bases is called shifting. The resemble of bits remaining after this basis reconciliation forms the shifted key. The shifted key generation rate is given by:

Rshifted = sRraw

Where's' is the shifting parameter, that is the fraction of bits for which the bases were the same. We get sh.ifted key to process further

5. Error correction

Error correction phase include two part first is error finding & second is either removing or correcting to the finding error.

STEP1- to find error we calculate pre error rate (PER).

The pre-error rate is realized by picking up little part RQT bits and comparing between Alice and Bob..Here PER=BER. For particular channel we get following BER shown in table 1

.

$$BER = \frac{N_{wrong}}{N_{total}}$$

……(1)

Where N_{wrong} is the number of bits in error and N_{total} is the number of bits received in total

STEP2- Error removing

1) Alice and Bob make replacements randomly & identically bits in their sifted keys and odd even checks some turns. In each turn, the exchanged string (part of sifted key) is divided to block in size M. The choice of M is very important to implement efficiency of protocol. To get perfect result M must chose in that manner so that the probability of an error occurrence is 1/2 per block .Then these bits must be discarded. The scheme needs only four times [10].

2) During each random permutation and block odd even comparison, these blocks will continue to be divided when the compared odd-even cannot be consistent as far as the errors are found, and then discarded. In order to avoid leaking information to attacker, Alice and Bob discard the last bit of each block, or discard the sub-block which odd-even lost. Because last bit is parity bit & the parity bits increase attacker's information on the key. [11]

3) After finishing four-time permutation and odd-even comparison, a random sub-odd-even comparison is carried out, which can take out any reserved errors. The process usually needs to perform twenty times [4], and the last bit of subset is also discarded during each odd-even comparison. It is proved in experiment that in each step of error removing, when the length of RQT is 1,000 bits, the percentage discarded errors is as follows: 60% are discarded in the first time, then about 25% RQT errors are discard in the second time, meanwhile about 7.5% are discovered and discarded in the third time, and only very little part, about 1% are discovered and discarded in the forth time. In fact, during error removing step, there is an RQT error fragment that is not removed without being discovered, which happens in discarding the last bit of each block or leak from sub-block. [11]

STEP3- Error Correction
After removing error there are still small error is present in some qubits. This error has to be corrected. In order to correct these errors we use two types of error correction codes for quantum computation. [4]

a. Bit-flip code

b. Phase-flip code.

The bit flip code changes the qubits of a corrupted state to correct the errors in bits and the phase flip changes the phase of a state to correct an erroneous phase of a state. According to Shannon's noiseless coding theorem

$$\lim_{n\to\infty}\frac{k}{n}=-e\log_2 e-(1-e)\log_2(1-e)\equiv h(e)$$

……..(2) Where

n = length of the sifted key

k = no of bit on which error correction is applied

e = error probability independently for each bit

6. Estimating attacker's information
Error free key is used in this process as input .Here we discuss two methodology use in this step.

a. Existing methodology

In emulation process, if the real Single-photon pulse is used on quantum channel to transfer key bits, Attacker cannot separate laser bean to eavesdrop the transmission on quantum channel. To Attacker, the only way is intercept-resend strategy. Here the bits number W that leaked to Attacker is about [8]

$$W=N(\frac{4}{\sqrt{2}})P+5\sqrt{N\left(4+2\sqrt{2}\right)P}$$

……. (3) Where

N = The length of RQT

P = The RQT pre-error rate

This estimated technique, state that the estimated number of information leaked to attacker is always less than in the fact.

b. Proposed Methodology for Estimating attacker's information

Recently we can use also calculate attackers mutual information IE [12]

$$I_E=1+\sum_{k=1}^{n}\left[\begin{matrix}\cos^2(\Phi_k)\log(\cos^2(\Phi_k))+\\ \sin^2(\Phi_k)\log(\sin^2(\Phi_k))\end{matrix}\right]$$

…… (4) Where

I_E = Mutual information

n = number of bases

Φ_k = angle between Alice's basis and basis in which attacker made measurements.

$\cos^2(\Phi_k)$ And $\sin^2(\Phi_k)$ are probabilities to measure unit

We can use this mutual information to estimating information of attacker. This research state that to reduce attacker' mutual info IE. We have to increase the no of bases (n)

7. Decision on continuation
After estimating attacker's information. We compare & analyze the result. For this we use "Quantum comparison circuit" & mathematical result. if there is any deviation from general behavior & specify range of mathematical result then there is attacker present between two authentic participant.. Then we abort the transmission and again start another new QKD process from beginning. If no attacker present we will continue for next step.

The second feature is the new opportunity for Eve detecting. When Alice's basis does not coincide with Bob's one Bob's bit is the same as Alice's with probability $\cos^2(\Phi_k)$ and his bit is wrong with probability $\sin^2(\Phi_k)$. But presence of attacker changes these probabilities in such a way that Alice and Bob should measure these changes.

8. Privacy Amplification

After decision on continuation one thing is very clear that the qubits we are receive now are error free , not altered by any attacker & these qubits will generate a secure quantum key. To increase the security further we use a additional step known as privacy amplification.

The role of the privacy amplification step is to Reduce the shrinking factor τ by which the error corrected key has to be compressed, given the error rate calculated in the error correction step and the bound on the amount of information leaked during the previous phases of the transmission, so that attacker's information about the final key is lower than specified value. To do privacy amplification we can use one of given methodology or we can use the combination of both methodology

a. First Methodology

In This calculation is performed using the methods by which we get length of final key (r) depends upon Various factor given eq (5)

$$r = n\tau - k - t \quad \ldots\ldots (5)$$

Where

n = length of the sifted key

k = number of bits disclosed during Error correction

t = security parameter

τ = shrinking factor

The key generation rate R in privacy amplification can calculate by given formula

$$R = R_{sifted}\left\{\tau + f(e)\left[\begin{matrix} e\log_2 e + \\ (1-e)\log_2(1-e)\end{matrix}\right]\right\}$$

……. (6)

In this method we increase the security by reducing the size (length) of final key.

b. Second Methodology

We can increase the security by applying quantum hash function. Let we get A string got from error removing step having length M. So we can calculate quantum hash function H(A). Here the length of H(A) is given by

$$H(A)length = M - W - s$$

…….(7)

Where

M =length of string

W =number bits that leaked to Attacker by Eq. (3)

s = Security coefficient

Large number of photons should be transferred if we need longer key , and the final length of the string is effected by the eavesdrop on quantum channel. During privacy amplification, the information intercepted by attacker is much less, even to one bit.

Quantum Key

After applying all these process (mentioned above) we get our final secured & unique quantum key. This quantum key provides us ultimate confidentiality & integrity. Because it is known only to authentic participant .This key can use anywhere to encrypt or decrypt to information. Key can also use for classical encrypt or decrypt methods as well.

Comparison

At last we compare our proposed model with existing model. Brief comparison is shown in table 1

Properties	**Proposed Model**	**Existing Model**
Authentication	√	×
Initialization	√	×
Quantum transmission	√	√
Error removing	√	√

Secrecy Enhancement	√	√
Decision on continuation	√	×
Steps required	9	5
Cost	More	Less
Time needed to Generate key	More	Less
Calculating mutual info	√	×
Ability discard process in middle	√	×
Difficult to bypass	√	×
Guarantee to Generate & Distribute correct key	√	×
wrong key generation	×	√
Attacker is detect before key generation & distribution	√	×
Use of classical channel	More	Less

Conclusion

Because of the existence of system losses and Attacker, the key cannot be formed and transferred simply by using existing model, which needs combined with non-quantum process & new methodology & several new step in QKD. Quantum key distribution protocol is improved in the paper, especially in the aspect of error removing, Authentication, Estimating Attacker's information & Privacy amplification. It will useful for deeper research in quantum key in the future while there have been substantial advancements in the field of quantum cryptography in the last decade, there are still challenges ahead before quantum cryptography can become a widely deployed key distribution system for governments, businesses, and individual citizens. Namely, these challenges include developing more advanced hardware to enable higher quality and longer transmission distances for quantum key exchange. Quantum cryptography is still in its infancy and so far looks very promising. This technology has the potential to make a valuable contribution to ecommerce and business security, personal security, and security among government organizations. If quantum cryptography turns out to eventually meet even some of its expectations, it will have a profound and revolutionary affect on all of our lives.

Refernces

[1] Wooters, W.K.: Zurek, W. H. (1982).A single quantum can not be cloned, Nature,Vol 299.

[2] Nielsen, M.A.; Chuang, I.L.(2002): Quantum Computation and Quantum Informtion, Cambridge University Press.

[3] Bouwmeester, D.; Ekert, A.; Zeilinger, A. (2000): The Physics of Quantum Information, Springer-Verlag, Berlin.

[4] Kitaev, A.Y. ; Shen,A.H.; Vyalyi, M.N.(2002) Classical and Quantum Computation, AMS.

[5] C.H.Bennett Experimental Quantum cryptography. Journal of Cryptology 1999; Vol.5

[6] Yang Yuguang, Some Opinion on Quantum Key Distribution Protocol[J].Communication Technology,Vol. 4,2002, pp. 1021-1024.

[7] A.C. Doyle, The Adventure of the Dancing Men , in The Annotated Sherlock Holmes, vol2, W.S.Baring-Gould, Wings Books, New Jersey, pp. 527-545 (1992).

[8] Charles Anthon, The first six books of Homer's Iliad with English notes, critical & explanatory, a metrical index, & Homeric glossary, Harper & Brothers, New York, p396.

[9] D.R. Stinson, Cryptography, Theory and Practice, CRC Press, Inc., Boca Raton, p. 4 (1995).

[10] H-K LO, H.F. Chau, and M.Ardehali, "Efficient Quantum key Distribution Scheme and a proof of its unconditional security". p396.

[11] Vladimir kur ochkinl, yurk kurochin. "Quantum Cryptography Security Improvement with additional states", ISBN 978-1-4244-6628-3/10/