ISSN 2349-6193
Impact Factor: 2.805

IJESMR

International Journal OF Engineering Sciences & Management Research

A REVIEW ON KEY DISTRIBUTION USING QUANTUM CRYPTOGRAPHY

Vijay Kumar*
*Faculty Member , FST Department, ICFAI University Himachal Pradesh

Keywords: Quantum Cryptography, Network Security, Quantum Key Distribution, Key Sharing

ABSTRACT

Cryptography in the past was used in keeping military information, diplomatic correspondence secure and in protecting the national security. However, the use was limited. Nowadays, the range of cryptography applications have been expanded a lot in the modern area after the development of communication means; cryptography is essentially required to ensure that data are protected against penetrations and to prevent espionage. Also, cryptography is a powerful mean in securing e-commerce. Cryptography is used to ensure that the contents of a message are confidentiality transmitted and would not be altered.

The encryption and decryption process is carried out with help of keys. Key sharing plays a very important role in the cryptography. In this research paper we explain the principle of quantum cryptography and quantum key distribution protocols

INTRODUCTION

In our modern age of telecommunications and the Internet, information has become a valuable thing. Sometimes it must therefore be kept safe from stealing - in this case, loss of personal data to an eavesdropper. There are many features to security and many applications, ranging from secure commerce and payments to private communications and protecting passwords. One important feature for secure communications is that of cryptography [1], which not only secure the data from stealing or modification, but can also be used for user authentication. The main aim of cryptography is to protect data transferred in the likely presence of an attacker. In cryptography, the data is converted into unreadable form, called ciphertext, that does not expose the original input. The cipher text can be reverse-altered by a designated recipient so that the original plaintext can be recaptured. The techniques of cryptography are usually categorized as conventional or current. Conventional techniques use operations of coding i.e. use of alternative words or phrases, transposition i.e. reordering of plaintext, and substitution i.e. alteration of plaintext characters).Whereas, current techniques use computers, and depends upon extremely long keys, convoluted algorithms, and intractable problems to achieve assurances of security. There are two main fields of modern cryptographic techniques: Public key encryption [2] and Secret key encryption [1],[2].A public-key encryption, in which a message is encrypted with a reciever's public key. The message cannot be decrypted by anyone who does not possess the corresponded private key, who is thus presumed to be the owner of that key and the person associated with the public key. A secret key is an encryption key known only to the party or parties that exchange secret messages. The risk in this system is that if either party loses the key or it is stolen, the system is broken. The development of quantum cryptography [3] was encouraged by the short-comings of classical cryptographic methods, which can be devided as either "public-key" or "secret-key" methods. Quantum cryptography is an approach to a cryptography based on the laws of quantum physics [4].

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 message. The word quantum itself refers to the most fundamental behavior of the smallest particles of matter and energy: quantum theory [5] 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.

The quantum cryptography depends on two important components of quantum mechanics-the Heisenberg Uncertainty principle and the principle of photon polarization . The Heisenberg Uncertainty principle[6] states that, it is impossible to determine the quantum state of any system without distributing that system. The theory of photon polarization states that, an eavesdropper cannot copy unknown qubits i.e. unknown quantum states, due to no-cloning theorem which was first introduced by Wootters and Zurek in 1982.

Quantum cryptography is thought to be secure for three main reasons [6]. One, the quantum no-cloning theorem states that an unknown quantum state cannot be cloned. Theoretically, messages sent using quantum cryptography would be in an unknown quantum state, so they could not be copied and sent on. Two, in a quantum system, which can be in one of two states, any attempt to measure the quantum state will disturb the system. A quantum message that is intercepted and read by an eavesdropper will become garbled and useless to the intended recipient of the message. Three, the effects produced by measuring a quantum property are irreversible, which means an eavesdropper cannot “put back” a quantum message to its original state. These three properties provide the power of quantum cryptography

QUANTUM KEY DISTRIBUTION

The best-known application of quantum cryptography is quantum key distribution (QKD)[7]. The goal of QKD is to allow two distant participants, traditionally called Alice and Bob, to share a long random string of secret (commonly called the key) in the presence of an eavesdropper, traditionally called Eve. The key can subsequently be used to achieve a perfectly secure communication and perfectly secure authentication , thus achieving two key goals in cryptography[8].

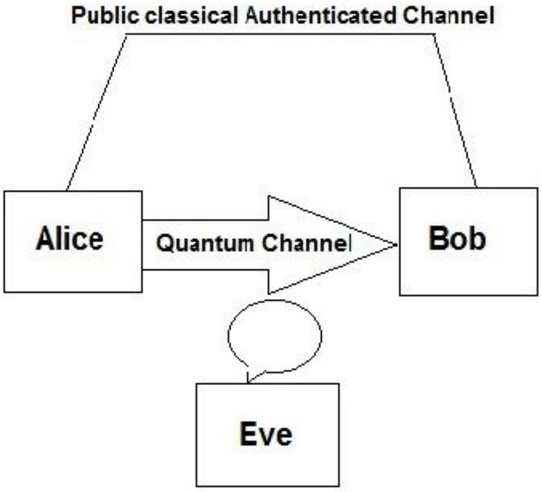

Fig.1 Quantum Key Distribution

Quantum key distribution comprises a quantum channel and a public classical authenticated channel[9]. As a universal convention in quantum cryptography, Alice sends quantum states to Bob through a quantum channel. Eve is suspected of eavesdropping on the line.

Quantum key distribution (QKD) uses individual photons for the exchange of cryptographic key data between two users, where each photon represents a single bit of data. The value of the bit, a 1 or a 0, is determined by states of the photon such as polarization or spin[10].

Quantum cryptography uses photons[11] to transmit a key. Once the key is transmitted, coding and encoding using the normal secret-key method can take place. But how does a photon become a key? How do you attach information to a photon's spin?

This is where binary code comes into play. Each type of a photon's spin represents one piece of information -- usually a 1 or a 0, for binary code. This code uses strings of 1s and 0s to create a coherent message. For example, 11100100110 could correspond with h-e-l-l-o. So a binary code can be assigned to each photon -- for example, a photon that has a vertical spin (|) can be assigned a 1. Alice can send her photons through randomly chosen filters and record the polarization of each photon. She will then know what photon polarizations Bob should receive.

When Alice sends Bob her photons using an LED, she'll randomly polarize them through either the X or the + filters, so that each polarized photon has one of four possible states: (|), (--), (/) or ( ). As Bob receives these photons, he decides whether to measure each with either his + or X filter -- he can't use both filters together.

Keep in mind, Bob has no idea what filter to use for each photon, he's guessing for each one. After the entire transmission, Bob and Alice have a non-encrypted discussion about the transmission[12].

The reason this conversation can be public is because of the way it's carried out. Bob calls Alice and tells her which filter he used for each photon, and she tells him whether it was the correct or incorrect filter to use. Their conversation may sound a little like this:

- Bob: PlusAlice: Correct
- Bob: PlusAlice: Incorrect
- Bob: XAlice: Correct

Since Bob isn't saying what his measurements are -- only the type of filter he used -- a third party listening in on their conversation can't determine what the actual photon sequence is.

Here's an example[13]. Say Alice sent one photon as a (/) and Bob says he used a + filter to measure it. Alice will say "incorrect" to Bob. But if Bob says he used an X filter to measure that particular photon, Alice will say "correct." A person listening will only know that that particular photon could be either a (/) or a ( ), but not which one definitively. Bob will know that his measurements are correct, because a (--) photon traveling through a + filter will remain polarized as a (--) photon after it passes through the filter.

After their odd conversation, Alice and Bob both throw out the results from Bob's incorrect guesses. This leaves Alice and Bob with identical strings of polarized protons. It my look a little like this: -- / | | | / -- -- | | | -- / | … and so on. To Alice and Bob, this is a meaningless string of photons. But once binary code is applied, the photons become a message. Bob and Alice can agree on binary assignments, say 1 for photons polarized as ( ) and (--) and 0 for photons polarized like (/) and (|).

This means that their string of photons now looks like this: 11110000011110001010. Which can in turn be translated into English, Spanish, Navajo, prime numbers or anything else the Bob and Alice use as codes for the keys used in their encryption.

The Importance Of Quantum Cryptography In The Real World

As mentioned in the section 3, before transmitting information QKD is exchanged to verify the agreed key combination. The advantage of QC over classical cryptography is that QC firstly a different medium of key distribution which is involved with photons, secondly by using a separate channel named as Quantum channel to distribute a large number of photons, and thirdly the mismatching orientation would be discarded without the actual results not been shared by the receiver.]

Through the above mentioned processors an eavesdropper would have a difficulty in identifying the real key distribution. If any case an eavesdropper is present in the middle firstly source and the destination which shared the orientation would not be the real one that the eavesdropper has, secondly due to the reason of mismatch orientation been discarded the real key distribution or the discarded orientation would not be accurate to the eavesdropper where statistically it is a 50-50 chance of getting it correct and thirdly if the eavesdropper does any change to figure out the correct key orientation photons would be destroyed where alerts would raise of destroyed photons.

The advantages mentioned above displays an error free communication along with more security and monitoring capabilities been involved which cannot be seen in classical cryptography.

Quantum Key Distribution Protocols

3.2.1 BB84 Protocol

Quantum key distribution algorithm described in BB84 protocol[14] utilizes any two orthogonal quantum states.Let us consider polarization states on single photon. Photon can be polarized rectilinearly(0 or 90 Degree) pr diagonally (45 or 135 Degree).One can correspond 0 and 45 Degree to binary-0 and 90 and 135 Degree to binary-1.this is called conjugate coding. Rectilinear and diagonal polarization of photons is the conjugate variables. As it is mentioned before, according to Heisenberg uncertainty principle, it is impossible to measure the values of any pair of conjugate variables simultaneously to any degree of accuracy.Each bit sent by Alice can be measured by rectilinearly or diagonally measurement devices ,but not both together.Meaning is either 0 or 1.And all the information about the photon can be lost.therefore it is impossible to measure it again.

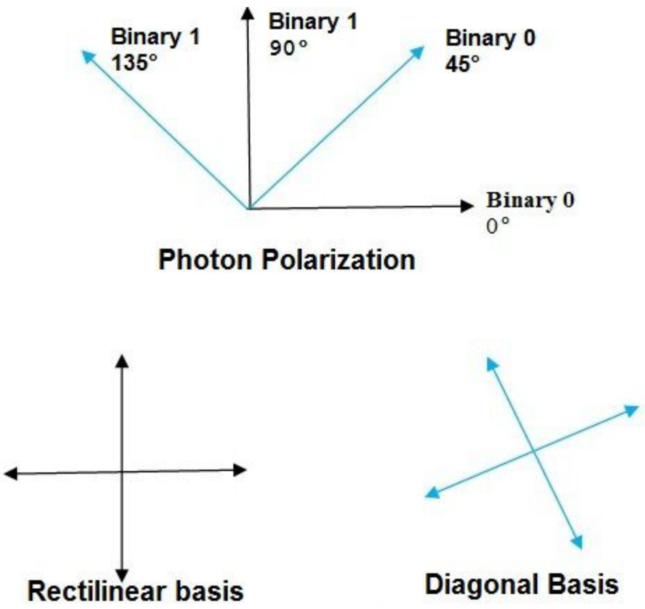

Fig. 2 BB84 Bit Encoding

If eve is trying to read the sequence that alice sent, she has to generate a new one and send it to Bob. But doing this Eve has to make assumptions on polarization of each photon what becomes a reason of distrubance.Because of it Alice and Bob will get different bits.

BB84 algorithm considers two steps of communication (one way communication- fro Alice to bob and two way public communication) and can be explained in a simple way [15]:

Step-1 One way Quantum communication

a) When Alice transmits a single bit,she takes a random sequence of orthogonal polarization (rectilinear or diagonally).She creates a sequence S of phtonos whose polarization directions represents bits in the original sequence.
b) Alice sends the sequence of phtonos S to bob.
c) For each photon Bob guess whether it was diagonally or rectilinearly polarized and measrues each bit with his assumption,producing a sequence of bits.As rectinlinear and diagonal polarization of photons are the conjugate variables according to Heisenberg uncertainity priniciple,it is impossible to measure values of their simultaeously to any degree of accuracy.

Step-2 Two way public communication

a) Communication through a public channel bob sends to Alice information on his measurement assumptions.than Alice sends to bob information which of bob's measurement assumption were incorrect.As a result incorrect measurements are deleted.
b) Alice and Bob communicate through a pubic channel to determine if evesdropping ook place.For there reason Alice and Bob select randomly a set of not deleetd bits and compare them.Discovered discrepancy proves that evesdroping took place.

3.2.2 BB92 Protocol

Soon after BB84 protocol was published, Charles Bennett realized that it was not necessary to use two orthogonal bases for encoding and decoding. It turns out that a single non-orthogonal basis can be used instead, without affecting the security of the protocol against eavesdropping. This idea is used in the BB92 protocol[16], which is otherwise identical to BB84 protocol.

The key difference in BB92 is that only two states are necessary rather than the possible 4 polarization states in BB84 protocol.

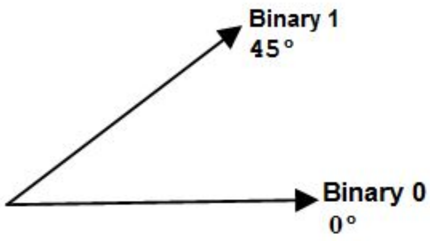

Fig. 3 BB92 2-States Encoding

As shown in figure 3, 0 can be encoded as 0 degrees in the rectilinear basis and 1 can be encoded by 45 degrees in the diagonal basis. Like the BB84 protocol, Alice transmit to Bob a string of photons encoded with randomly chosen bits but this time the bits Alice chooses dictates which bases Bob must use. Bob still randomly chooses a basis by which to measure but if he chooses the wrong basis, he will not measure anything; a condition in quantum mechanics which is known as an erasure. Bob can simply tell Alice after each bit Bob sends whether or not he measured it correctly.

LIMITATIONS OF QUANTUM CRYPTOGRAPHY

For now, computers capable to transmitting information using quantum cryptography are very large, custom-made and, thus, expensive. A couple of banks have already taken advantage of this security method, but few other organizations would be able to afford it in the foreseeable future.

With regards to entangled photons, which seem to be absolutely safe, there is also a serious practical problem not only with the cost, but also with keeping them entangled long enough to meet the needs of the real world. While the system is perfect in theory, it is going to be very hard to implement it in practice.

Another problem is that for distances beyond 50 kilometers or so, the noise becomes so great that error rates skyrocket. This not only leaves the channel very vulnerable for eavesdroppers, but also makes it virtually impossible to send information. However, it is potentially possible for quantum keys to be exchanged through the air in the future. Tiny telescopes would then have to be aligned to detect the signal. Some calculations even suggest that photons could be detected by a satellite, which would allow communication between continents.

CONCLUSION

In this paper an aspect of the workings of quantum cryptography and quantum key distribution technology is presented. This technology is basically depends upon the polarization of photons, which is not a well regulated quantity over long distances and in multi-channel networks.

Securing data and data communication is a top priority because the consequences of unsecure data can have grave effects on both the economy and national security. Classical key distribution systems are protected only by the limitations of the currently available computing power. But with the increased computing power of Quantum Computers, classical cryptography is no longer a fully secured communication method. Quantum Cryptography provides more security level then any classical cryptosystem as quantum computing works according to the laws of quantum physics and does not depend on hard mathematical functions. Hence, the resulting Quantum Cryptosystem is more secure and cannot be cracked easily.

REFERENCES

1. *Charles H Bennett, and Gilles Brassard, 'Withdrawn: Quantum Cryptography: Public Key Distribution and Coin Tossing', Theoretical Computer Science (2011).*
2. *Patrick Bellot , Toan-Linh-Tam Nguyen, Minh-Dung Dang, Quoc-Cuong Le, Thanh-Mai Nguyen "Usages of Secure Networks built using Quantum Technology", Intl. Conf. in Computer Science, Can Tho, Vietnam – RIVF'05, February 21–24, 2005.*
3. *N. Benletaief, H. Rezig, and A. Bouallegue, 'Reconciliation for Practical Quantum Key Distribution with Bb84 Protocol', in Mediterranean Microwave Symposium (MMS), 2011 11th, 2011), pp. 219-22.*

4. *Han Zheng-Fu, and Li Hong-Wei, 'Security of Practical Quantum Key Distribution System', in Intelligent Signal Processing and Communications Systems (ISPACS), 2011 International Symposium on, 2011), pp. 1-3.*
5. *R. J. Hughes, J. E. Nordholt, D. Derkacs, and C. G. Peterson, "Practical free-space quantum key distribution over 10 km in daylight and at night,"New Journal of Physics, vol. 4, pp. 43.1–43.14, 2002.*
6. *I. B. Damg°ard, S. Fehr, L. Salvail, and C. Schaffner. Cryptography in the bounded quantum-storage model. Research Series RS-05-20, BRICS, Department of Computer Science, University of Aarhus (www.brics.dk), 2005.*
7. *Anand Sharma, Vibha Ojha, R.C.Belwal, Vishal Goar "Quantum cryptography – The Concept and challenges " in proceeding of 2nd International Conference on Computer and Automation Engineering (ICCAE 2010) Singapore, volume 1, 2010 pp. 710-714*
8. *Kartalopoulos, S.V."Identifying vulnerabilities of quantum cryptography in secure optical data transport" milcom 2005, vol 5, pp. 2788-2796*
9. *Dierks, T. and E. Rescorla, "The Transport Layer Security (TLS) Protocol Version 1.1", RFC 4346, April 2006.*
10. *G. Brassard, N. Lütkenhaus, T. Mor, and B. C. Sanders, "Limitations on practical quantum cryptography," Phys. Rev. Lett., vol. 85, pp.1330–1333, 2000.*
11. *R. Perlner and D. Cooper, "Quantum Resistant Public Key Cryptography: A Survey", Proc of IDtrust 2009, Gaithersburg, MD, Apr. 14-19, 2009.*
12. *Mohamed Elboukhari1, Mostafa Azizi2 and Abdelmalek Azizi, "IMPROVING TLS SECURITY BY QUANTUM CRYPTOGRAPHY" International Journal of Network Security & Its Applications (IJNSA), Vol.2, No.3, July 2010*
13. *M. Elboukhari, M. Azizi, A. Azizi, "Analysis of Quantum Cryptography Protocols by Model Checking", IJUCS, Vol 1, pp. 34-40, 2010.*
14. *Holger F Hofmann , Toshiki Ide "Optimal cloning of single-photon polarization by coherent feedback of beam splitter losses" New Journal of Physics vol .8 , pp. 130.1-130.9, Aug 2006*
15. *Applied Cryptography, Second Edition: Protocols, Algorithms, and Source Code in C (cloth) Author(s): Bruce Schneier*
16. *Anand Sharma , Vibha Ojha "Quantum Cryptography with photon pairs" in International Journal of Engineering Science and Technology (IJEST) Volume 2 Issue 7 july 2010 pp. 3320-3325..*