The International Journal Of Engineering And Science (IJES)
||Volume||3 ||Issue|| 2||Pages|| 06-09||2014||
ISSN(e): 2319 – 1813 ISSN(p): 2319 – 1805

A Review on BB84 Protocol in Quantum Cryptography

[1,]Shiji Johny , [2,] Anil Antony
[1,2,]*Department of Computer Science & Engineering Jyothi Engineering College,Cheruthuruthy*

---ABSTRACT---
The implementation of secure keys, as we know is done by an important cryptographic technique called Quantum cryptography.The popularity of Quantum Key Distribution increases day by day due to it's unrivaled security level. Quantum Mechanics principles in particular Heisenberg Uncertainty principle helps in achieving this high security level which is promised.This review paper deals with the working principle of the famous Quantum cryptographic protocol , BB84 as well as the key distillation methods for establishing the secure cryptographic keys through an unsecure channel. .

INDEX TERMS: *Quantum Cryptography,Quantum Key Distribution,BB84 Protocol*

Date of Submission: 5 February 2014 Date of Acceptance: 05 March 2014

I. INTRODUCTION

Now a days,the popularity of the Quantum cryptography growing rapidly.The implementations of Quantum key Distribution will provide new network services.Mainly the cryptographic techniques are widely used when the security becomes an important issue.If we want to communicate secretly to other persons in a network,we have to ensure that the network is a secure one.Here comes the importance of the various cryptographic techniques.The security of the cryptographic techniques depends on the security of the keys which are used for encrypting the message or information.Normally different mechanisms are used for creating these secure keys.But the Quantum key distribution will provide more secre keys than the keys which are provided by the existing cryptographic techniques. Currently,Quantum communication over long distances is an important issue due to the problems The maximum distance of successful Quantum Key Distribution is currently over 200km.The bit rate of Quantum Key Distribution systems reaches a few Mbits/s in a typical telecom metro politan area network.It is even possible to achive Quantum Key Distribution between the Earth and low Earth Orbit (LEO) satellites equipped with retroreflectors[3].

Until recently,.the end users of the Quantum Key Distribution techniques are banks,big corporations and public administrations etc.The major reason behind this is the large implementation cost of the Quantum cryptography technology.The additional implementation costs of these technology are due to two elements: additional optic fiber to establish a quantum channel ,and the quantum devices to send and receive quantum bits.The security provided by the quantum technologies is regarded as the highest level of data protection.The end users can access the services and devices supporting quantum cryptography.Now a days ,the modern network services support by the Quantum key distribution ,but the users cannot personalize the service according to their needs.There fore,customers should be able to measure the security offered by the quantum based solutions and choose the right level of the data protection.This paper consists of mainly two parts:introduction to quantum cryptography and the description of the BB84 protocol.The key distillation processes are also described.

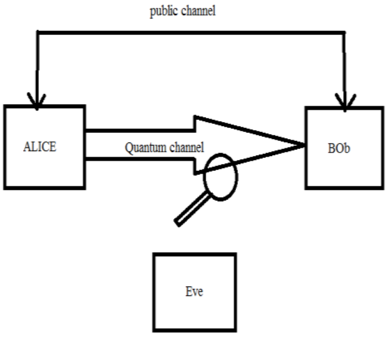
II. QUANTUM CRYPTOGRAPHY

The data confidentiality is the basic requirement when we communicate within a network.This data confidentiality is ensured by the cryptographic technique.This makes the message in to an unreadable form for others excepting the sender and the receiver.Symmetric key cryptography is the most popular technique use today for ensuring data confidentiality.In this cryptographic method,encryption and the decryptions are performed by the same key.So there must be a sharing of the secret key.The agreement or distribution of the secret key between the sender and receiver may lead to the data confidentiality.

The current key agreement protocols like Deffie-Hellman key agreement protocol can be used to establish the secret key .But they are vulnearable to some types of attacks.For avoiding these attacks,the proposed best solution is the Quantum Key Distribution.Quantum cryptography is in fact that symmetric key cryptography with Quantum Key Distribution(QKD)[3]. Basically the Quantum cryptography is similar to the traditional cryptography.In Quantum cryptography the qu antum information qubits (quantum bits)are used for creating the keys instead of bits in the traditional cryptography[6].There are two possible values 0 and 1are used for representing the qubits.Basic Quantum mechanics rule Heighsenberg uncertainty principle is used in the quantum cryptography.The QKD distribution is based on the polarization of the photons.Single photons are used in the BB84 protocol.These photons are used for creating the quantum keys.

III. QUANTUM KEY DISTRIBUTION

Quantum key distribution is a key agreement method which is introduced by quantunm cryptography.This is used for distributing an encryption key for symmetric ciphers and not for transmitting the data between the sener and receiver.The law of Quantum Mechanics will provide a high level of security.Because these ensures that any measurement modifies the state of the transmitted quantum bit. The fig(1) represents the Quantum Key Distribution.As like the traditional cryptography ,the quantum cryptography also have the sender and receiver Alice and Bob.They want to send a secret data.So they must share the secret key.Here the Quantum Key Distribution have two types of channels :public channel and a quantum channel.A quantum channel which is used for transmitting the qubits with the information abiut the distrubuted key.The public channel is used by the end users for check whether the communication through the quantum channel is distorted.

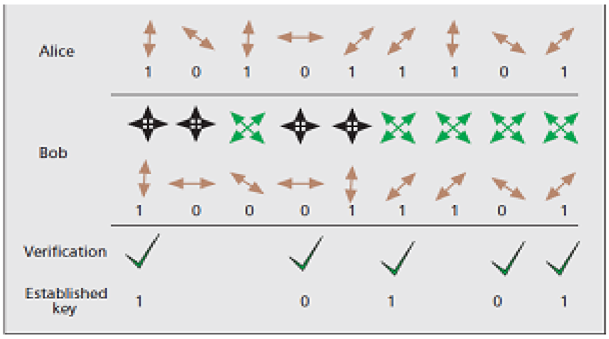


Fig(1)

Normally ,in the experimental setup the polarizing filters are used for creating the photons. Polarizing filters are materials that allows only light of a specified polarization direction to pass. Polarizing filters uses the phenomenon polarization.Polarization can be used to represent a 0 or 1.detectors are also used for detecting the photons on the receiver side[4].Usually the quantum channels are optic fibers and the public channels are internet.

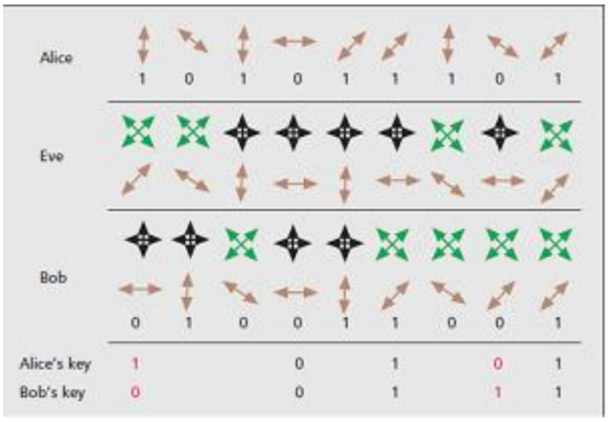
IV. BB84 PROTOCOL

We all know that several QKD protocols are present .But the most popular is still BB84.This protocol is invented by the Bennett and Brassard in 1984.Hence the BB84 protocol.It is based on the information encoded using the polarization of the photons. As like in the traditional cryptography,BB84 protocol also uses three characters :Alice(usually the sender),Bob(Usually the receiver),and Eve(The eaves dropper).Alice and Bob want to communicate secretly by establishing a cryptographic key.Eve wants to gain information about this key.Before establishing a new key between Alice and Bob ,they both have to define two alphabets.They are rectilinear and diagonal.Assume that the rectilinear alphabet photons with horizontal polarization 0 degree means the bit 0 and photons with vertical polarization 90 degree means the bit 1.Similarly in the diagonal alphabet ,photons with polarization with -45 degree means the bit 0 and photons with polarization 45 degree means bit 1.Bob can only able to perfectly measure the polarization 0 degree and 90 degree in rectilinear basis and photons with -45 degree and 45 degree in the diagonal basis. Fig(2) represents the key establishment using BB84 protocol without eavesdropping..In fig(2),two crossed double headed arrows (green arrows) means the diagonal basis.Similarly ,two crossed double –headed arrows (black arrows) means the rectilinear basis.



(Fig 2)

At the start of the protocol ,Alice sends Bob a string of bits ,which is encoded by the polarized photons(qubits).Alice sends these bits to Bob using randomnly chosen alphabets rectilinear or diagonal through the quantum channel.Bob receives these bits using the rectilinear basis or diagonal basis .The Bob also chooses the basis randomnly.But Bob informs Alice which basis is he used for measurement through the public channel.Only the basis is discloses and the measurement result is kept secretly.Alice also informs Bob ,which basis is she used for measuring the photon's polarization.During the checking of the basis,they keep only the bits corresponding to the right basis.Other bits are discarded.So the new key consists of those bits for which Bob has chosen the basis correctly.Then Alice and Bob have the same string of bits.The new key is called sifted key[base].In the fig(2) ,the first photon is detected perfectly and will be the first bit of the new key.Alice and Bob have to reject the second and third bits because Bob chose the wrong basis,and the measured polarization is uncertain.The fourth bit is detected perfectly and will be the part of new key.This algorithm ensures that the the distributed key consists 50% of the bits sent by Alice.The remaining bits must be rejected. Fig(3) represents the eaves dropping in the BB84 protocol.Asume that the Eve is eaves dropping in the quantum channel during communication between the sender and the receiver.For obtaining the information,Eve has to measure the polarization of the photons using the two alphabets :rectilinear or diagonal.if the basis chosen by the Eve is wrong,then the polarization will be changed.This is present in the fig(3).Originally,the first bit has vertical polarization ,but Eve evesdrops using a diagonal basis.So the photon has the 45 degree polarization.After the Bob's measurement,this photon has a horizontal polarization and will be decoded as 0.So here Alice sent a vertically polarized photon and Bob selected the correct rectilinear basis,but they obtain different bits.So Alice and Bob compare the part of the key,they uncover the eavesdropping Eve.Here the passive eavesdropping is not possible.When an eve tries to evedrops on photons,she will change the quantum states of the photons.Eve is not able to clone an unknown state of the photon.Therfore,BB84 protocol provides a high level security.



Fig(3)

The Quantum Key Distribution is only a part of the key establishment process.There may be a chance to occur numerous errors in the string of bits received by the Bob.The errors may due to the eavesdropping and the disturbance in the Quantum channel etc.We can not identify separately the errors ,whether due to eavesdropping or not .so we are considering all errors as eaves dropping errors.

The end users must calculate the error rate and decide whether the eaves dropper is present or not.For this they can compare a small portion of the key and calculate Quantum Bit Error Rate (QBER)using the formula: QBER=Number of errors/Total number of bits*100% If the error rate is greater than the threshold value ,then the entire key is discarded.Otherwise key distillation process is performed for avoidind errors.The first key distillation method is reconciliation.For doing this,sender and receiver divide the key into blocks and compare the parity of each block.If the parity does not agree,the error is present.For avoiding these errors they divide each blocks in to two and repaeat this process untill the errors have been corrected.After reconciliation the length of the key is reduced.The second method is privacy amplification .For making the key as a more secure one,some of the bits are rejected for reducing the Eaves information about the distributed key

V. RELATED WORK

The QKD implementations are in progress.Mainly the end users of the QKD techniques have been banks,big corporations,and public administrations.The major reason behind this is the cost [3].The maximum distance of successful QKD transmissions is currently over 200 Km.The bit rate of QKD systems reaches a few Mbit/s.The QC service is already implemented to secure bank transactions in Switzerland.The QC technology is also implemented in different networks.The most famous protocol used in these networks is still BB84. DARPA is the Quantum network which is implemented by Harvard University in 2004.SECOQC(Secure Communication Based On Quantum Cryptography) is a network implemented in Vienna. The main goal of the SwissQuantum network, installed in the Geneva metropolitan area in March 2009, was to validate the reliability and robustness of QKD in continuous operation over a long time period in a field environment.The QC technology will provide high security level and can make it is easier to meet specific end-user security requirements

V. CONCLUSION

Quantum Key Distribution is a better solution for providing a key agreement between the sender and the receiver.The QKD is used with the the symmetric key cryptography,will provide a better solution for ensuring highest level of security.BB84 protocol is most popular protocol currently used for implementing the Quantum Key Distribution.The fundamental rules of Quantum Mechanics will provide the better security for Quantum cryptography.The passing Eves dropping is not possible in the QKD.New implementations of QKD will provide new network services.

REFERENCES

[1] G. V. Assche, *Quantum Cryptography and Secret- Key Distillation* (Cambridge Univ. Press, 2006)

[2] Srinivasan Arunachalam,*Quantumkey Distribution:A Resource Letter(*International Journal of computer Applications(0975-8887)Volume37-N0.3,January 2012)

[3] Andrzej R.Pach,and Marcin Niemiec,*Management of Security In Quantum Cryptography(*IEEE communications Magazine,August 2013).

[4] Douglas Stebila, Michele Mosca ,"The Case for QuantumKeyDistribution"*http://eprints.qut.edu.au/(*Workshop on Quantum and Classical Information Security, Vico Equense,Italy,26 October 2009)

[5] M.Niemiec,*Quantum Cryptography-The Analysis of SecurityRequirements(*Int'l.conf.Transparent Optical Networks, S Miguel,Portugal,2009).

[6] Anton Zeilinger, *Quantum Information* (2005).

[7] Charles H.Bennett,and Gilles Brassard,*Quantum Cryptography:Public key distribution and Coin tossing*(International Conference On Computers ,Systems and Signal Processing,Bangalore,India December10-12-1984).

[8] D.L Guptha,and Hitesh Singh,*Quantum Cryptography Using BB84 Protocol(2009).*