ISSN: 0974-2115
www.jchps.com Journal of Chemical and Pharmaceutical Sciences

An efficient implementation of BB84 quantum key distribution protocol

Sarath R*, Shajin Nargunam A
Department of Electronics and Instrumentation Engineering, Noorul Islam University, Kumaracoil-629180 Tamil Nadu, India.
***Corresponding author: E-Mail: sarathraveendran@gmail.com**

ABSTRACT

A new approach for improving the efficiency of BB84 protocol for Quantum Key Distribution is proposed in this paper. One of the most effective factors in Quantum cryptography is that it ensures ultimate security. This paper explains how the data required for key making can be effectively sent through both quantum channel and classical channel. The usage of dual channel technique for key making are analysed which ensure the way to remove the practical difficulties of quantum cryptography. This paper provides a new mechanism for improving the key length and thereby improving the efficiency of BB84 protocol.

KEY WORDS: Quantum Key Distribution, quantum channel, Qubits.

1. INTRODUCTION

Communication with effective security has been the ultimate need of the users. In cryptography, key is exchanged by physical means. Key send by physical means has many practical security problems which leads to the major setback in cryptography. Quantum cryptography provides a solution for the above issue. In Quantum cryptography keys are transmitted in the form of photon using quantum channel. The advantage of Quantum cryptography is that it has not only two states but also a superposition of both known as qubit. The most successful topic in quantum cryptography is quantum key distribution. BB84 is the protocol most widely used for quantum key distribution. BB84 protocol was put forth by Bennett and Brassard (1984). This protocol assures a secure communication using quantum mechanics. This protocol uses quantum channel for transmitting the photons and the public channel for cross examining the transmitted photons. Quantum mechanics has the property of identifying the presence of intruder. Quantum cryptography is theoretically strong but has practical difficulties.

Quantum key distribution: Quantum cryptography differs from the classical cryptography because quantum cryptography is developed by two principles. Quantum cryptography works on two principles: First one states that without disturbing the system, it is not possible to measure a quantum state. Other principle is no-cloning which states that quantum state can be copied only after destroying it. Quantum cryptography uses secure channel to transmit a polarized photon which then will create the secret key. This secret key generated from a form of a random string of bits. These bits then will be used as a secret key in a conventional cryptography scheme. BB84 allows a secret key to be agreed between two communication parties without having two parties meet face to face. BB84 allows receiver and sender to establish a secret common key sequence using polarized photons.

BB84 protocol: In 1984 Charles Bennett and Gilles Brassard published the first QKD protocol [BB84]. BB84 protocol transfers key using two channels: quantum channel and public channel. Each photons are transmitted after polarising the photons using four polarization state (0º, 90º, 45º and 135º). Each of these photons are in a state denoted by one of the four following symbols: —, |,⁄, \,.

BB84Protocol consists of five steps:

a) Raw Key Extraction
b) Key Shifting
c) Key Distillation
d) Error Correction
e) Privacy Amplification

Raw Key Extraction: Sender and Receiver exchange some quantum states + –. Quantum information is passed along a quantum channel from Sender to be measured by Receiver, with or without the presence of eavesdropper.

Key Shifting: Sender and Receiver decide between them which of the measurements will be used for the secret key with the help of classical channel.

Key Distillation: Key distillations are used to repair information losses through the channel.

Error Correction: A classical error-correction protocol estimates the actual error rate of the transmission, known as the Quantum Bit Error Rate (QBER).

Privacy Amplification: This is designed to counteract any knowledge Eavesdropper may have acquired on the raw key. Privacy amplification compresses the key material by an appropriate factor, determined by the previously calculated QBER.

Draw backs of existing system: During the sifting process, receiver transmits information over the public channel to sender regarding the basis that he measured for each bit. Sender then responds with a yes or no answer. Mismatched bits are identified and removed. In 1999, Ardehali, Chau, and Lo published an optimization for the sifting process that can potentially result in increased thorough put (Ardehali, Chau, & Lo, 1999). As opposed to an

unbiased method of choosing and measuring bases, the authors recommend using a biased method for choosing the bases. Given that the probability of sender and receiver choosing matching bases is

$$p=\sigma 2+ (1- \sigma) 2 \quad (1)$$

Where σ is the probability of choosing one basis and (1- σ) is the probability of choosing the other basis. By increasing the probability that both sender and receiver choose matching bases, fewer bits are lost through sifting, and throughput, or key rate, is increased. Unfortunately, it is also possible for Eavesdropper to bias her measurement choice and increase her probability of choosing the same basis as Sender sends. This lead to the modified proposed method.

Error may occur during the photon transmission because of long distance travel. The transmission length, the data rate, and the quantum bit error rate are the three important factors of quantum key distribution. According to Quantum Bit Error Rate (QBER) and raw key rate a general formula could be arrived. Key rate is the product of pulse rate υ, average no of photons per second μ, the transfer efficiency η_t, and detector efficiency η_d

$$R_{raw} = \frac{1}{2}\upsilon\eta_t\eta_d \quad (2)$$

The fraction of bit loss due to error correction is given as

$$r_{ec} = QBER\left(\frac{7}{2} - log_2 QBER\right) \quad (3)$$

And the fraction of bit loss due to privacy amplification as

$$r_{pq} = 1 + log_2\left(\frac{1+4QBER-4QBER^2}{2}\right) \quad (4)$$

So the final bit rate is

$$R_{final} = (1 - r_{ec})(1 - r_{pq})R_{raw} \quad (5)$$

The transmission length, the data rate, and the bit error rate (BER) are the three important factors of novel key distribution. Estimation of the fraction of bit loss due to error correction as

$$r_{ec} = QBER(\frac{7}{2} - log_2 QBER) \quad (6)$$

And there is no fraction of bit loss due to privacy amplification. So the final bit rate is

$$R_{final} = (1 - r_{ec})\left(1 - r_{pq}\right)R_{raw} \quad (7)$$

As transmission length l increases, transfer efficiency η falls rapidly down, which in turn causes more errors in raw key and a decrease in the final bit rate to zero. So the maximum transmission length could be computed.

2. PROPOSED METHOD

In this paper, a two-way key distribution protocol is proposed. In this method sender and the receiver will not be able to know the secret key until the last step when they finish the comparison of their bases. This proposed method, is considering how to involve quantum technique and classical technique in the key distribution process. Extracting the advantages of both Quantum cryptography and Classical cryptography a new concept has been introduced in our method, This method uses three channels Channel A, B and C. Channel A is the quantum channel which transmits data in the form of photons and B is the dedicated channel between sender and receiver, where data are transmitted in digital form. Channel C is the open channel (eg) internet.

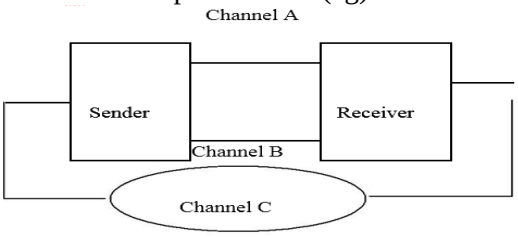


Fig.1.Schematic representation of proposed model

In this method key is generated by combining two stages. During the first stage data to be sent are split into two halves and the data are sent separately through quantum Channel and classical channel. Sender selects half the random classical bits and random orthogonal bases. The selected bits and bases are used to generate qubits. The qubits are transmitted to receiver through the quantum channel. Once the receiver have received the qubits, sender and receiver must exchange the random bases through public channel in order to measure the received qubits and transfer them to ordinary bits. Sender and receiver keeps are record to indicate the correct and incorrect positions of the received bits. This data is taken as the half of key. During the second stage half the data transmitted through the dedicated channel is taken. Here the data are selected on the basis of previous orthogonal bases. This data is taken as the other half of the key. First stage and second stage is repeated several times depending on the key size and the required level of accuracy. After the completion of the required rounds, key is generated.

Proposed BB84 protocol works as follows: a) Sender and Receiver are in need of a secret key generation. b) Random bits are generated by sender and receiver independently. These bits are then divided in to two equal halves. c) One half of the random bit is then passed through polarizer by the sender. Polarizer is of two type's

rectilinear and diagonal polarizer. d) Depending on senders choice each random bit is polarized and send to the receiver. e) Now the receiver will accept the each bit depending on its own polarization choice. f) Sender and Receiver will announce their polarization base using classical communication through channel C. g) Sender and Receiver perform an error correction procedure on the data using classical communication through channel C. h) Now the sender and receiver will compare their raw data and common bits are taken as the key 1. i) Now the sender will send other half of the random data through channel B. j) Receiver will only select the random data based on the previous polarization base and the selected data is taken as key 2. k) Key 1 and key 2 is taken as total key.

Mathematical model: To determine the probability that a qubit is not changed after the measurement by the receiver in the required rounds, we need to calculate the probability of the following:

a) Sender and receiver choses the same base and result is correct.

b) Sender and receiver choses wrong base and result is correct.

c) Sender and receiver choses right base and result is wrong.

Calculating the probability that during n number of rounds the observed qubit will not change is achieved by calculating the probability of measuring the qubit in all possible states using the correct base and the other two states using the wrong base. The probability of the error is given in (8).

$$P = \left(\frac{1}{4}\right)^n \times \left(\frac{1}{4}\right) \times \left(\frac{1}{4}\right) = \left(\frac{1}{4}\right)^{n+2} \qquad (8)$$

Since sender and receiver choose the two bases with the same probability, the probability of sender and receivers basis compatibility is $\left(\frac{1}{4}\right)\left(\frac{1}{4}\right) + \left(\frac{1}{4}\right)\left(\frac{1}{4}\right) = \left(\frac{1}{4}\right)$ so half of the bit will be thrown away. Hence the total probability is given by

$$P = \left(\frac{1}{4}\right)^{n+2} + \left(\frac{1}{4}\right) \qquad (9)$$

From (8) we can calculate the probability of the correct value when the considering key size of m bits as calculated in (10).

$$C = \left(1 - \left(\frac{1}{4}\right)^{n+2}\right)^m + \left(\frac{1}{4}\right) \qquad (10)$$

Selecting the key size affects the number of rounds required to be performed to achieve the required accuracy. Considering various key size and 99% target accuracy, the required rounds will be as given in the table.

$$\frac{(n+2)\log\left(\frac{1}{4}\right)}{\log\left(\frac{1}{4}\right)} = \frac{\log(1-m.\overline{99})}{\log\left(\frac{1}{4}\right)} + .25 \qquad (11)$$

Table.1.Key generation in novel method

Sender sends random sequence of photons through quantum channel A	+	+	**x**	+	**X**	**x**	**X**	+	+	+	**x**	**x**
Polarizations of photons sent by SENDER	+	+	x	+	X	x	X	+	+	+	x	x
Measurement types made by RECEIVER	+	+	+	+	X	x	X	x	+	x	x	+
Results of RECEIVER's measurements	V	H	H	H	A	D	A	D	H	D	A	H
RECEIVER publicly tells SENDER which type Of measurement he made On each photon	+	+	+	+	X	x	X	x	+	x	x	+
SENDER publicly tells RECEIVER which measurements were the correct type	YES	YES	NO	YES	YES	YES	YES	NO	YES	NO	YES	NO
SENDER and RECEIVER each keep the data from correct measurements And convert to binary (Data 1)	1	0		0	1	0	1		0		1	
Sender sends random Sequence of binary bits through quantum channel B	1	1	0	0	1	1	1	1	1	0	0	0
SENDER and RECEIVER each keep the data from correct measurements (Data 2)	1	1		0	1	1	1		0		0	
Key (combine Data 1, Data 2)	1001010111011100											

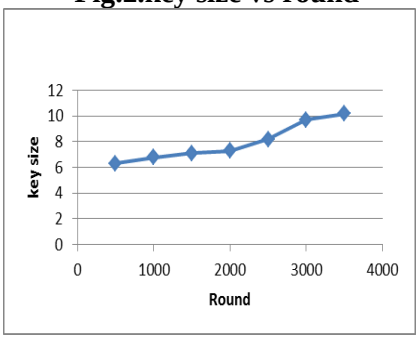
In classical cryptography the probability of bit received is 100% which means bit rate error is 0%. But the breakage of classical algorithm is highly possible since the key transfer is very much insecure. Hence in classical cryptography the probability of hacking is unknown and is equal to 0%security. In our proposed system the bit rate error is reduced to 0% and security increases to 70% as dual channel is employed and transmission delay is calculated. The selection criteria at the receiver do not depend entirely on the rectilinear and diagonal bases, but are taken on

the basis of combination factors. In the authentication process, where we employ dual channel to transmit the hashed keys, the intercept/ resend attack by Eve is eliminated by two criteria. One by verification that the sender is genuine and the other by calculating the time delay between the receipts of hashed keys at the receiver. Either of these parameters determine whether a third party was present at the middle or not, and thus avoiding the probability of impersonation.

Table.2.Keysize vs round

Key size	Round
500	6.3
1000	6.8
1500	7.1
2000	7.3
2500	8.2
3000	9.7
3500	10.2
4000	11

Fig.2.key size vs round



3. CONCLUSION

In this proposed system the bit rate error is reduced and security is increased with the help of dual channel. By combining the advantages of quantum techniques and classical techniques a try has been made to implement a novel technique to ensure secure key communication.

REFERENCES

Bennet C.H, Brassard G, Quantum Cryptography: Public Key Distribution and Coin Tossing II Proc. of IEEE Int. Conf. on Comput. Sys. and Sign. Proces., Bangalore, India, 1984, 175-179.

Bennet H, Bessette F, Brassard G, Salvail L, and Smolin J, Experimental Quantum Cryptography, Journal of Cryptography, 5, 1992, 3-28.

Imtiaz Ahmad, Shoba Das A, Hardware implementation analysis of SHA-256and SHA-512 algorithms on FPGAs, Computers and Electrical Engineering, 31, 2005, 345–360.

Kurochkin V.L, Protocols for quantum cryptography, Micro/Nanotechnologies and Electron Devices (EDM), 2011 International Conference and Seminar of Young Specialists on, 2011, 114,115.

Nielsen M.A, and Chuang I.L, Quantum Computation and Quantum Information, Cambridge University Press, 2002.

Robert P Mc Evoy, Francis M Crowe, Colin C Murphy, William P Marnane, Optimisation of the SHA-2 Family of Hash Functions on FPGAs, 2013 IEEE Computer Society Annual Symposium on VLSI (ISVLSI), 2013, 317-322.

Shannon C.E, Communication Theory of Secret Systems II Bell Syst., Tech. Jour., 28, 1949, 658-715.

Stallings W, Cryptography and Network Security Principles and Practice, Second Edition, Prentice Hall International, 1999.

Stephen Barlett, Lecture on quantum computing, NITP Summer School, Adelaide, Australia, 2003.

Vignesh R.S, Sudharssun S, Kumar K.J.J, Limitations of Quantum & the Versatility of Classical Cryptography: A Comparative Study, Environmental and Computer Science, 2009. ICECS '09, Second International Conference on, 2009, 333-337.

Zhizhong Yan, Meyer-Scott E, Bourgoin J, Higgins B.L, Gigov N, Macdonald A, Hubel H, Jennewein T, Novel High-Speed Polarization Source for Decoy-State BB84 Quantum Key Distribution Over Free Space and Satellite Links, Lightwave Technology, 31 (9), 2013, 1399-1408.