ISSN (ONLINE): 2395-695X
ISSN (PRINT): 2395-695X

International Journal of Advanced Research in Biology, Engineering, Science and Technology (IJARBEST)
Vol. 1, Special Issue 5, May 2013

DUAL CHANNEL TECHNIQUE FOR QKD

R.Sarath
Department of Electronics and Instrumentation Engineering
Email:sarathraveendran@gmail.com

Dr.A.Shajin Nargunam
Department of Computer Science and Engineering
Email: ashajin@yahoo.com

Noorul Islam University Kumaracoil-629180
Nagercoil-629003. Tamilnadu, India

ABSTRACT

A new approach for the implementation of Quantum Cryptography is proposed in this paper. Quantum Cryptography has practical weakness like lack of authentication, single photon generation and many real time implementation problems. This paper explains how the drawback of BB84 protocol is eliminated by combining Classical Cryptography and Quantum techniques. We analyze the usage of Dual Channel Interferometer technique and thereby fusing Quantum techniques with classical technique. And their combination result in the feasibility of authentication, and hacker identification, thereby introducing a novel method of QKD transmission.

Keyword: Quantum Cryptography, BB84, Classical Cryptography.

1. INTRODUCTION

Secure Communication has become the topmost priority of modern society. Quantum Cryptography was proposed in 1984, since then there has been significant development in it. Quantum Cryptography is an approach for secure data communication by applying the principles of quantum physics [1,4]. The most successful topic of Quantum Cryptography is Quantum Key Distribution (QKD) which was first introduced by Bennett and Brassard in 1984. the most important aspect of Quantum Cryptography is that quantum system has *"qubits"* which not only has two states ie '0' or '1' but also a superposition of both. QKD is a theoretically strong but has lot of practical drawbacks. major drawback of QKD is very difficult to implement digital signature or authentication scheme. Another drawback of QKD is that there is always a possibility of change in polarization of photons. Similarly it is very difficult to generate single photon.

The basic objective of the paper is to point out the practical difficulties in implementing QKD and to provide a solution to overcome the practical difficulties of QKD and thereby utilizing the whole potential of QKD.

2. QUANTUM KEY DISTRIBUTION

QKD is the most successful application of Quantum Cryptography. QKD is now a commercially available technology, which is used to send random sequence of polarized form of photons between such and receiver[5]. The security of QKD lies on the fact that the polarized form of photons on rectilinear and diagonal basis cannot be measured by Eve. This unconditional security is guaranteed by the laws of quantum physics. Various protocols have been proposed in Quantum Cryptography such as BB84, B92 & EIR [2,4]. In Classical Cryptography keys are generated by mathematical computation are proving to be insecure.

3. BB84 PROTOCOL

BB84 protocol was proposed by Bennett and Brassard. According to this protocol two channels are required for QKD, one quantum channel and the other public channel. Alice sends photons to Bob using quantum channel and they use public channel to agree on the key. Alice sends Bob randomly polarized photon through the quantum channel. For each photon chooses either rectilinear or diagonal orientation and inform the type of orientation to Alice through public channel. Bob measure the photons on the basis of information obtained through public channel and makes the raw key. Error may appear during raw key generation because of noisy environment or long distance travels are eliminated with the help of public channel. No eavesdroppers can obtain the information from Quantum channel because the data are transmitted in the form of photons.

In this work the feasibility of Quantum cryptography over classical cryptography is analysed. Extracting the advantage of both the techniques a new concept has been introduced. In Quantum cryptography the existence of eavesdroppers can be realized on analyzing the photons. But the generation of single photon is very difficult.

ISSN (ONLINE): 2395-695X
ISSN (PRINT): 2395-695X

International Journal of Advanced Research in Biology, Engineering, Science and Technology (IJARBEST)
Vol. 1, Special Issue 5, May 2013

With the help of interferometric technique the presence of eavesdroppers can be identified. Here the data is divided into two equal halves and one half is taken as D1 and other half as D2. Now data D2 is further divided into two equal halves named D2a and D2b. D2a and D2b are encrypted using any of the classical cryptography algorithm and keys are generated. Let K1a and K2b are the keys of D2a and D2b respectively. Now using the two channels encrypted data are sent. D2a is sent through channel 1 and D2b through channel 2 and their keys k1a and k2b are transmitted through opposite channel. Using interferometric technique the receiving time of data through two channels can be calculated. If the delay exceeds the threshold value using a feedback channel, the transfer of data D2 is stopped. Thereby Quantum Stratagem is implemented and the presence of eavesdroppers is identified.

An evolved plan for QKD employs the use of programming polarizer. This technique uses two quantum channels (quantum channel 1 and 11 for key distribution)

Quantum key distribution has a programming polarizer and a key store. The secret key is generated with the help of programming polarizer (PGP).Output from the PGP is mixed signature data, providing authentication and is fed as input to the LASER with help of mixer. Amplified data is then made to pass through the quantum channel 1. Data equivalent to the above data is then made to pass through the quantum channel 2. The two data are received using same type of receiver and the data is synchronized. The delay times between the two keys are calculated using delay time circuit. If the delay is above the critical value then the transmission of the key will be stopped using a feedback circuit.

If there is no delay then the QKD has been successfully send. QKD and the signature data is then separated using separater. Similar process will take place from the receiving section also. Analyzing the keys both Alice and Bob can come to a common conclusion for generating the original key.

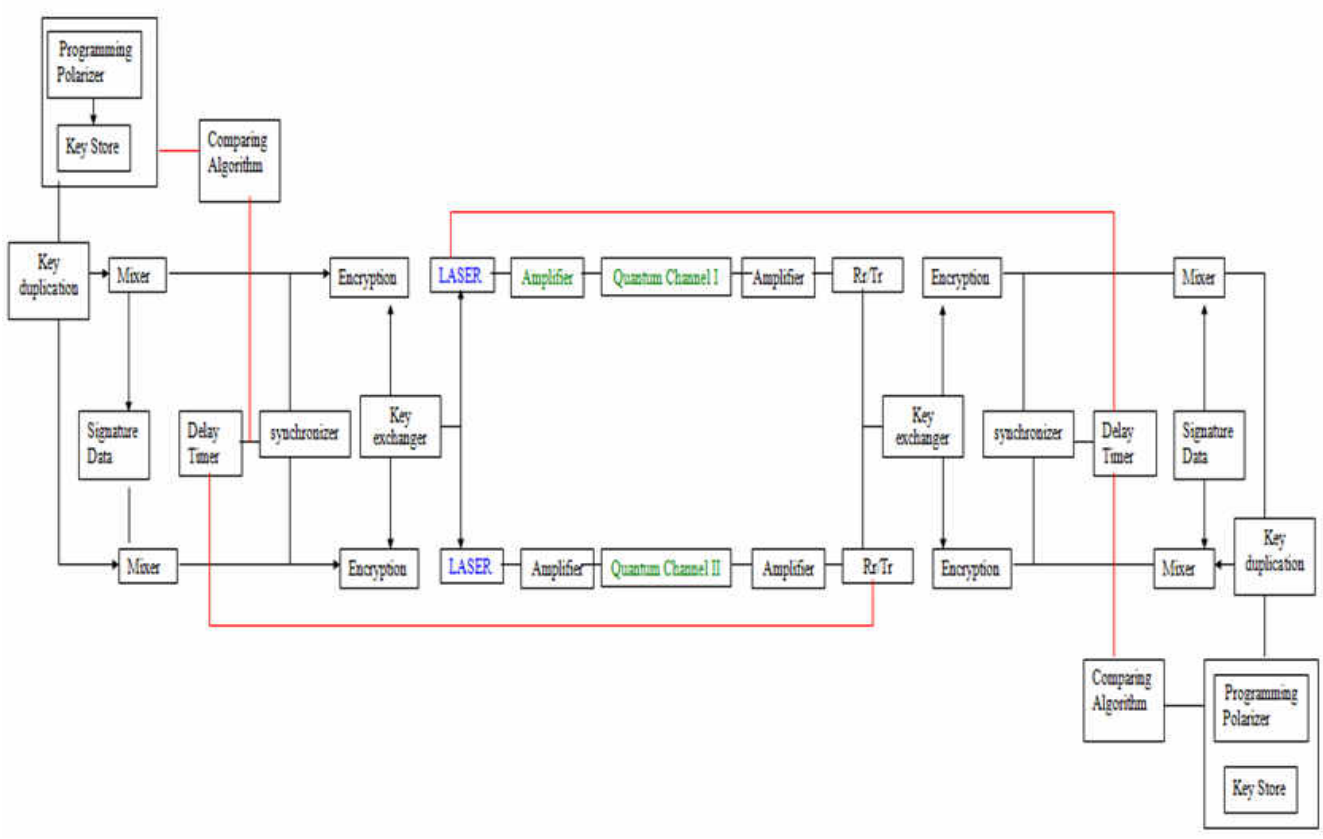

Figure-1 Proposed QKD Model

ISSN (ONLINE): 2395-695X
ISSN (PRINT): 2395-695X

International Journal of Advanced Research in Biology, Engineering, Science and Technology (IJARBEST)
Vol. 1, Special Issue 5, May 2013

4. AUTHENTICATION SCHEME

The security of the transmitted message is enhanced by improving its integrity. In the former methods of quantum cryptographic communication, there is no provision for confirming that the message has come from a genuine source. In the proposed system, authenticity of the sender is verified. That is, Bob can verify that the received message was sent by Alice only and not any other third party hacker.

The proposed system uses two special channels connected in parallel from the sender to the receiver for conveying information. These special channels are the quantum channels through which the authenticated key is split and sent. This key is used to decode the message received through public channel.

The authentication process of the key, as in fig.1 is done by splitting it into two equal parts K1 & K2 and producing a hash value H1 & H2 for both keys respectively by using hash algorithm. It is then followed by combining the hash value H1 with the opposite key K2, and the hash value H2 with the other key K1, and thus creating a pair of authenticated keys K2H1 & K1H2 respectively. After the concatenation, the first pair K2H1 is sent through the 1st quantum channel and the second pair K1H2 through the 2nd quantum channel.

At the receiver, it's checked if both the pairs are received without any delay. After which they are subjected to verification process. Hash values #1 & #2 are generated again for the keys obtained at the receiver by the same hash algorithm. If the received and the generated hash values are equal, the message is said to be authenticated or else the communication is aborted. Two factors like time delay and bit rate error have been taken into account while transmitting keys. These are determined by using the principle of interferometric technique.

In simple expression,
If H1= #1,
H2= #2,
Then message is authenticated.
Else
Communication aborted.

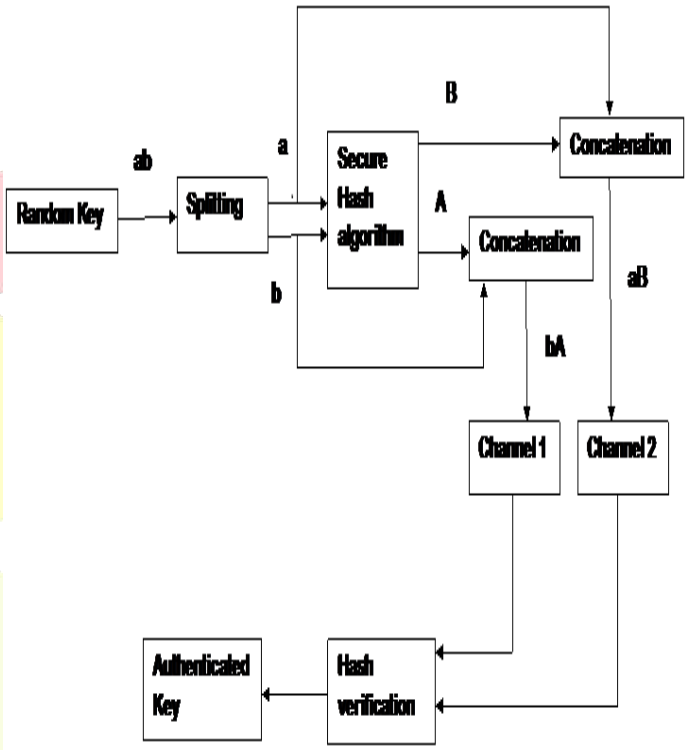

Figure 2 Improved Authentication Scheme

The purpose of using two quantum channels increases security by avoiding the probability of eves dropping. Intercepting the information from one channel does not provide the complete key information and thereby eliminates the intercept/resend attack (i.e. eve pretends to be Alice or Bob and intercepts communication)

4.1. Practical Implementation

4.1 Key generation

ISSN (ONLINE): 2395-695X
ISSN (PRINT): 2395-695X

International Journal of Advanced Research in Biology, Engineering, Science and Technology (IJARBEST)
Vol. 1, Special Issue 5, May 2013

Figure 4.1 Key generator output

The output of each block has been explained with figure as follows. First block is Random key generator. The generated random key has shown below. The key generated is ' **vfcp**'. Here the Random key generator is designed to generate key having four character.

4.2 Key word splitting

Figure 4.2 First half of the key word

The key generated is given to key split block and it split the key word into two equal halves. The first half is vf , it has been shown on the dialog box below.

4.3 Encrypted key word

Figure 4.3 output of encryption block

The first half of the key word is subjected to the encryption process. The figure below shows the output of the encryption block. This encryption is done using another key generated by a random key generator

Figure4.4 Second half of the key word

The figure shows the second half of the key k1 generated. This forms the second channel.

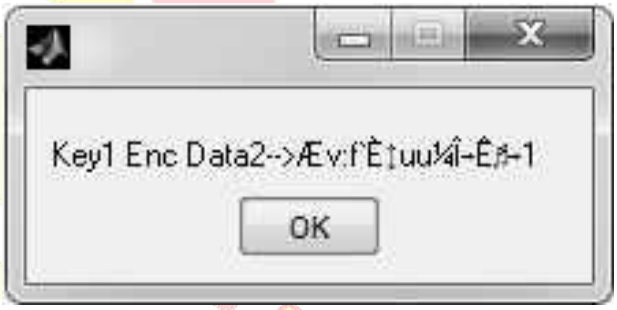

Figure 4.5 second half of key word encrypted

The second half of the key is also subjected to encryption in channel 2. This has been encrypted using a key generated in the channel 2.

4.4 Data at communication channel

Now the encrypted data of the first half, second half and the key generated to encrypt both the data has to be send to the receiver through a proper communication channel. Two channels are properly choosed and the first half of key 1 encrypted and key used to encrypt the second data are mixed together using a time division multiplexer. The combined data is further subjected modulation. Similarly the second half of key encrypted and the key used to encrypt the first half forms channel 2. The figure shows the contents of channel1 and channel 2.

It is very clear that each channel consists of two set of data and these two data has to be transmitted together

ISSN (ONLINE): 2395-695X
ISSN (PRINT): 2395-695X

International Journal of Advanced Research in Biology, Engineering, Science and Technology (IJARBEST)
Vol. 1, Special Issue 5, May 2013

in the same channel. A multiplexer can be utilized to accomplish this task.

Figure 4.6 content of data transfer on communication channel

A multiplexer (or MUX) is a device that selects one of several analog or digital input signals and forwards the selected input into a single line. There are different type of multiplexers are available such as time division multiplexer and frequency division multiplexer. The time division multiplexing is utilized here for the data transmission.

4.5Binary signal of encrypted data

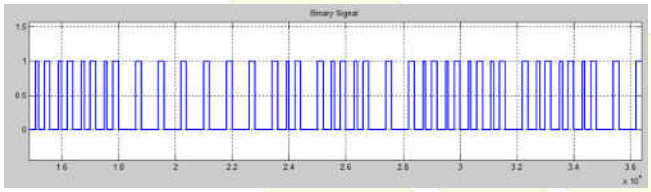

Figure 4.7 digital signal corresponding to encrypted data

The encrypted data is converted into digital signals. The equivalent digital signal in the channel one has been shown below. This binary signal is send through the channel by using suitable modulation technique.

4.6 Modulated signal

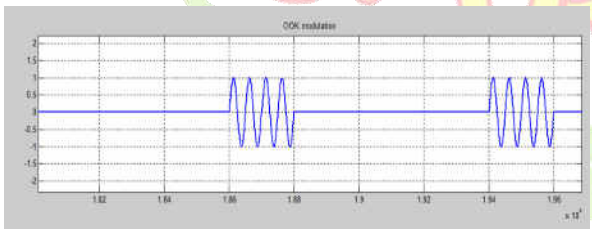

Figure 4.8 Modulated signal

The digital signal has been send through the communication channel. The digital signal is further subjected to the modulation. The modulation technique used here is on off keying modulation. The figure below shows the output of on off keying modulated signal of the channel 1.

4.7 keyword retrieved at receiving end

Figure 4.9 Regenerated key at receiver side (first half)

The modulated signal is received at the receiver end. This modulated signal is demodulated and output of the demodulated signal is rearranged by a demultipluxer. The encrypted data and key are separated. Both this data are given to decryption block. It decrypts the first part of the key, which shows in the figure below.

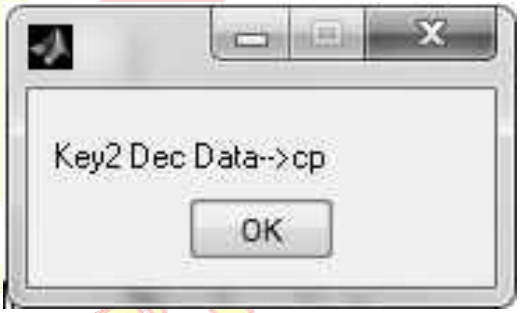

Figure 4.10 Regenerated key at receiver side (second half)

The figure below shows the decrypted output of the second part of the key. The second part of the key under goes same decryption process. After decryption the second half of the key word retrieved as shown.

The above figure shows that both halves of the key k1 has been retrieved back without any damage. The two portions of the key words has to be joined together to form the key k1

ISSN (ONLINE): 2395-695X
ISSN (PRINT): 2395-695X

International Journal of Advanced Research in Biology, Engineering, Science and Technology (IJARBEST)

Vol. 1, Special Issue 5, May 2013

Figure 4.11 Key 1 at receiving end

As soon as the key k1 reaches the receiver side, it generate another key k2 in a random generator present at the receiver end. This key k2 transmitted from receiver end to sender end. The process of the data transmission is same as the key k1. Now both the receiver side and the sender side have both the keys k1 and k2. This two keys are subjected to a same comparing algorithm at both the ends and form a third k3. This key k3 is used for the encryption of plain text into cypher text.

6. CONCLUSION

We have proposed a simple scheme for quantum key distribution utilizing two quantum channels. Dual channel implementation helps in implementing authentication in quantum BB84 protocol. We combined the advantages of quantum techniques and classical techniques and tried to implement a novel technique to ensure secure communication.

7. REFERENCES

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

[2] Bennet C.H. Quantum Cryptography Using any Two1Nonorthogonal States II Phys. Rev. Lett., 1992, V.68, pp. 3121-3124.

[3] Wooters W.K., Zurek W.H. A single quantum cannot becloned II Nature. 1982, V.299

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

[5] Mohamed Elboukhari, Abdelmalek Azizi, Mostafa Azizi, Implementation of Secure Key Distribution Based on Quantum Cryptography, IEEE, 2009.

[6] W.Stallings, Cryptography and Network Security Principles and Practice, Second Edition, Prentice HallInternational, 1999.US NIST.

[7] Imtiaz Ahmad, A. Shoba Das; Hardware implementation analysis of SHA-256and SHA-512 algorithms on FPGAs. Computers and Electrical Engineering 31(2005) 345360.

[8] S NIST, Secure Hash Standard, Draft FIPS PUB 180-2,May 2001.

[9] Robert P. McEvoy, Francis M. Crowe, Colin C. Murphy and William P. Marnane, Optimisation of the SHA-2 Family of Hash Functions on FPGAs Department of Electrical Electronic Engineering, University College Cork, Ireland.

[10] S.M.Barnett & S.J.D.Phoenix, "Securing a Quatum Key Distribution Relay Network using Secret Sharing," IEEE GCC Conference and Exhibition, Dubai, February 2011.

[11] Yang Zhang, Wei Chen,Hong-Wei Li, Hong-Wei Li, Shuang Wang,Zheng-Fu Han,Quantum Secret Sharing of Key in networks IEEE,2011.