A Novel Hybrid Technique for Secret Key Sharing in Networks

R. Sarath
Assistant Professor
Department of Electronics & Instrumentation
Noorul Islam University
Kumaracoil- 629180

A. Shajin Nargunam , Ph.D
Professor
Department of Computer Science
Noorul Islam University
Kumaracoil- 629180

ABSTRACT
A new approach for secret sharing of key in networks is proposed in this paper. Secret key sharing is an important problem in cryptography. This paper explains how secret key can be safely transmitted by combining Classical cryptography and Quantum techniques. The usage of dual channel technique and programmable polarizer are analyzed which ensure the way to remove the practical difficulties of quantum cryptography. This hybrid combination result in feasibility of authentication and hacker identification there by introducing a novel method for secret key transmission.

Keywords
Classical Cryptography, Quantum techniques, Authentication, Hacker.

1. INTRODUCTION
Secure communication has become the most important need of the modern society and its developments are increasing dramatically. To make this secure transmission of data, cryptographic techniques have been used. In Classical Cryptography, keys are generated by mathematical computation or logical techniques. No one can assure the security of the key that is send via physical means. This leads to the major failure in classical cryptography. Quantum cryptography overcomes this disadvantage by sending the key in the form of photon using quantum channel.[1]. The most important aspect of Quantum cryptography is that quantum system has qubits which not only has two states ie '0' and '1' but also a superposition of both. Various protocols have been proposed in quantum cryptography such as BB84, B92, EIR etc [2]. BB84 protocol was first proposed by Bennett and Brassard. According to this protocol two channels are required for key transfer one quantum channel and one public channel. Sender measures the photons on the basis of information obtained through public channel and makes raw key. Quantum cryptography is theoretically strong but has lot of practical difficulties [3]. Few drawbacks of Quantum Cryptography are implementing authentication schemes, generating single photon, possibility of change in polarization of photons. But the major drawback of quantum cryptography is that it is very difficult for long distance photon transmission. Hence both the cryptographic technique does not provide solution for key transfer.

The basic objective of this paper is to put forth a new technique by combining the advantages of Quantum cryptography and classical cryptography there by introducing a new technique for secret key transmission.

2. BB84 PROTOCOL
BB84[4] allows a bit string to be agreed between two communications parties without having two parties to meet face to face. BB84 allows the receiver and sender, to establish a secret common key sequence using polarized photons. Each of these photons is in a state denoted by one of the four following symbols: —, |, ⁄, \, According to [1], the first two photon states are emitted by a polarizer which is set with a rectilinear orientation and the other two states are emitted by a polarizer which is set with a diagonal orientation.

If the receiver wants to obtain the secret key as it is sent by the sender, then the receiver needs to receive each photon in the same polarised state.

To exchange a secret key in BB84 protocol, Sender and receiver must do the following:

Sender creates a binary random number and sends it to receiver using randomly two different bases + (rectilinear) and ×(diagonal). Receiver simultaneously measures the polarization of the incoming photons by randomly using the different bases. Here the receiver does not know which of his measurements are deterministic. Later, the sender and receiver communicate the list of the bases they used via public channel. This communication carries no information about the value of the measurement, but allows sender and receiver to know which values were measured by receiver correctly.

Receiver and sender keep only those bits that were measured correctly and will discard those sent and measured in different bases. If the 50 % of the bases are same then the receiver agree with sender bits and, hence they can reconstitute the random bit string. In other case they may think that the information channel was eavesdropped.

Error may appear during the raw key generation 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

$$R_{raw} = \frac{1}{2}\upsilon\eta_t\eta_d \qquad \text{Eq(1)}$$

Tancevski[18] has estimated the fraction of bit loss due to error correction as

$$r_{ec=QBER}\left(\frac{7}{2} - log_2{}^{QBER}\right) \qquad \text{Eq(2)}$$

And the fraction of bit loss due to privacy amplification as

$$r_{pq} = 1 + \log_2(\frac{1+4QBER-4QBER^2}{2}) \quad \text{Eq(3)}$$

So the final bit rate is

$$R_{final=}(1-r_{ec})(1-r_{pq})R_{raw} \quad \text{Eq(4)}$$

As the transmission distance increases the quantum transmission efficiency decreases. Presence of disturbances in the channel decreases receiving efficiency. More over single photon generation is very difficult. Practical implementation of quantum key distribution has lot of hurdles like long distance transmission, and high QBER. Hence a new method has been proposed.

3. NOVEL METHOD

Extracting the advantages of both the techniques a new concept has been proposed. This proposed work considers 3 channels, Channel A,B and C.

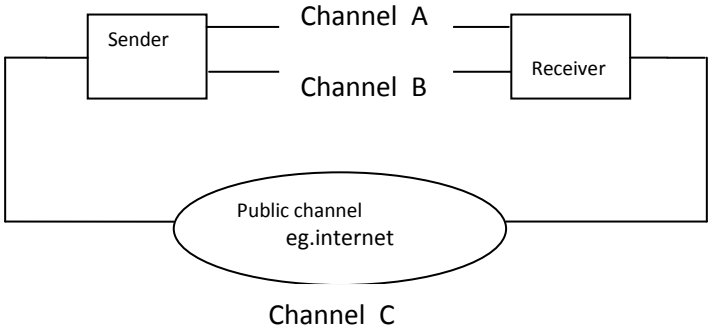

Fig 1 Simple Architecture of proposed method

Channel A and B are the dedicated channel between sender and receiver. Channel C is the open channel (eg) internet. Bit string is then made to pass through the programmic polarizer. In programmic polarizer there are two bases one bases representing rectilinear polarization and other representing diagonal polarization. In rectilinear polarization there are two states (0º, 90º.). For representing 0º state binary value of S is selected and for 90º state complement of S is selected. In diagonal polarization there are two states (45º, 135º.).

For representing 45º state binary value of P is selected and for 135º state complement of P is selected. For each bit,the sender can select any one of the bases depending on his choice. After selecting the base, the sender can select any one of the state . If the sender select the rectilinear base, then the data along with the state, is then send through the channel A. If sender selects the diagonal base, then the data along with the state is then send through the channel B . Receiver will receive the data from both the channels. Receiver will generate its own choice of bases and corresponding states. And send the states to sender through the dedicated channel. This whole process is known as raw key extraction.

Table 1. Key Generation in Transmission Section

Step	Bit Sequence	2	2	3	3	5	5	7	7	9
1	Sender logic sequence	001	001	010	010	101	101	111	111	10001
2	After passing through receiver filter	s	s	s	s	s	s	p	p	p
3	Senders state	S001	S001	S010	S010	S101	S101	P111	P111	P10001

Receiver will compare each states. If both the states matches that bits will be selected. Then the bits will be compared. Same bit will be selected. Otherwise that bit will be discarded. This process is known as key error correction. Now the sender and receiver will compare their raw data and common bits are taken as the secret key.

Table 2. Key Generation in Receiving Section

Step	Bit Sequence	1	2	3	4	5	6	7	8	9
1	Sender logic sequence	000	001	010	011	101	110	111	100	10001
2	After passing through senders filter	S	p	S	s	s	p	p	s	s
3	Senders state	s000	p001	s010	s011	s101	p110	p111	s100	s10001

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

$$r_{ec=}BER(\frac{7}{2} - log_{2}^{BER}) \quad \text{Eq(5)}$$

so the final bit rate is

$$R_{final}=(1-r_{ec})\ R_{raw} \quad \text{Eq(6)}$$

Table 3. Comparison table for features of various cryptographic algorithm

Features	Classical cryptography Algorithm	BB84	Novel Method
Authentication	**Yes**	**No**	**yes**
Need dedicated channel	**No**	**yes**	**yes**
Distance transmission	**Longer**	**Short**	**longer**
Bit rate error	**Lower**	**higher**	**lower**
Key transfer	**Insecure**	**secure**	**secure**

4. NOVEL BB84 PROTOCOL

1. Sender and Receiver are in need of a secret key generation

2. Sender and Receiver generate independent secret sequences of random bits. Random bits are then divided in to two equal halves

3. Sender now allows the one half of the random bit to pass through programming polarization (P.G). P.G has two choices representing rectilinear and diagonal polarizer .Sender can select its own choice of representation

4. S and S bar represent 0º, 90º polarization respectively P and P bar represent 45º and -45º polarization respectively.

5. Depending on senders choice each random bit is combined with polarization representations

6. Now sender selects the value for S and P. If S=0 then P=1 . so automatically Sbar will become 1 and Pbar become 0 and If S=1 then P=0 .so automatically Sbar will become 0 and Pbar become 1

7. Sender will now send the two half of the random bit combined with polarization representations through two channels to the receiver

8. Same operation will be performed by receiver using other secret sequences of random bits and will send the two half of the random bit through two channels to the sender

9. Using classical communications to identify which half of the random subsequence of shared secret bits have to be selected first

10 Sender and Receiver will announces their own S and P value

11. Sender and Receiver perform an error correction procedure on the data using classical communication

12. Sender and Receiver if select opposite value for S and P then data will be discarded otherwise resulting data is the raw key

13. Now the sender and receiver will compare their raw data and common bits are taken as the secret key

5. CONCLUSION

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 quantum cryptography Sender and Receiver chooses two bases which are rectilinear bases and diagonal bases. Since Sender and Receiver use different bases half of the photons are discarded, so the probability of bit received will be only 50%. Another disadvantage of QC is single photon generation and detection is possible only to small extent . This will again reduce the QC bit rate gain. In this proposed system the bit rate error is reduced to 0% and security increases 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

By combining the advantages of quantum techniques and classical techniques a try has been made to implement a novel technique to ensure secure communication.

6. REFERENCES

[1] 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, ecember 1984, pp. 175-179

[2] Bennet C.H. Bessette F. Brassard G. et.aI. Experimental Quantum Cryptography J.Cryptology II 1992, V. 5.

[3] Mohsen Sharifi1 and HooshanAzizi,"A Simulative Comparison of BB84 Protocol with its Improved Version",JCS&T Vol. 7 No. 3,PP. 204-208.

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

[5] 299Shannon C.E. Communication Theory of Secret SystemsII Bell Syst. Tech. Jour., 1949, V. 28, PP. 658-715.

[6] 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, Journal of* , vol.31, no.9, pp.1399,1408, May1, 2013

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

[8] US 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] Stephen Barlett, "Lecture on quantum computing," NITP Summer School, Adelaide, Australia, 2003.

[11] M. A. Nielsen and I. L.Chuang, "Quantum Computation And Quantum Information," Cambridge University Press, 2002.

[12] W. Stallings, Cryptography and Network Security Principles and Practice, Second Edition, Prentice HallInternational, 1999.US NIST, Descriptions of SHA-256,

SHA-384 and SHA-512, http://csrc.nist.gov/encryption/shs/sha256-384-5I2.pdf , 2001.

[13] Implementation ofSecure Key Distribution BasedOn Quantum Cryptography

[14]Quantum Cryptography For Secure Satellite Communications, Richard J. Hughes*, William T. Buttler, Paul G. Kwiat, Steve K. Lamoreaux,

[16]Chaotic Quantum Cryptography Stamatios V. Kartalopoulos,The Fourth International Conference on Information Assurance and Security

[17] 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, Journal of* , vol.31, no.9, pp.1399,1408, May1, 2013.