ISSN No: - 2456 – 2165

End to End Encryption Using QKD Algorithm

Ajith.B[1]
Department of EIE
Bannari Amman Institute of Technology
Erode-Tamilnadu
Ajith.Ei15@Bitsathy.Ac.In

Deepa.R[2]
Department of EIE
Bannari Amman Institute of Technology
Erode-Tamilnadu
Deepar@Bitsathy.Ac.In

Abstract—Today nearly all of the people are involved in communicating each other with the help of online communication. Nearly three fourth of the world are connected via social media.So it is very important to secure the data transmission between the user. And in addition to this future of computer's will be of by Quantum technologies. So the In this paper we are going to see how to increase the security of online transmission through Quantum shift distribution algorithm. In this paper idea outlines the implementation of this most advanced level of encryption by Quantum Key Distribution method and importance of quantum cryptography in future.

Keywords: - Quantum Cryptography, Online Security, Quantum Key Distribution (QKD)

I. INTRODUCTION

We have seen lot of communication portals in digital network but the securities of those portals are mean do much to the people. If there occurs any breach in security numerous data of our properties will be washed out. Though there are lot of encryption methods available today, that gives high level security such as in online payment procedures, sharing important document via social media, military related communication. Everything that are send via digital communication is encrypted [1]. Today there are various types of encryptions are being used, like AES, RSA. In encryption a plaintext is modified into different character and numbers, which is then transmitted in communication channel. The converted text is called cipher text, this is again converted back to original plain form when received. Between the transitions key holds a major role for converting the cipher text.the future of digital communication relay on the quantum computers. When quantum computers hold a place in day to day life, the encryption methods available today will be no longer safer. So Quantum cryptography pays way for the ultimate security.It is based on the law of physics[2]. Ensuring privacy between the two parties. One of the leading social application Whats app is using end to end encryption which is through RSA algorithm.But when quantum computers comes in place of present one, RSA method algorithm lacks accuracy and leads to leakage of data between communication. So the importance of quantum cryptography is in hike to reduce the shortcoming accompanied in present methods. One of the major advantage of Quantum key distribution is that when a third party is trying to get data between transition automatically sender gets alert , so that breach is broken down. Even Switzerland protects its valuable vote by Quantum Encryption [4].

Quantum key distribution (QKD) is one of the algorithms that can be implemented to strengthen the security portal. It uses quantum mechanics property to generate random secret key for guaranteeing secure communication. The random secret key is used to encrypt and decry-pt the text message. As said QKD has the property of detecting third party trying to access the key.

II. METHODOLOGY

QKD involves sharing random it sequence between sender and receiver. The probability for eavesdroppers to make absolute breach those bits is very low. Random bits are employed as tool to encrypt and decry-pt text message between two parties. Because everything send is being converted to photons as shown in Figure 1.

For instance two parties are taken Alice and bob.When Alice sends a message at random value, and if Bob to chooses card of same random value message is display, otherwise he reads completely wrong. When bob reads the complete photons, shifting takes place to transfer data. Sends random basis setting to both parties to fond which is correct. Each value is checked and remaining values are kept for raw key material.

ISSN No: - 2456 – 2165

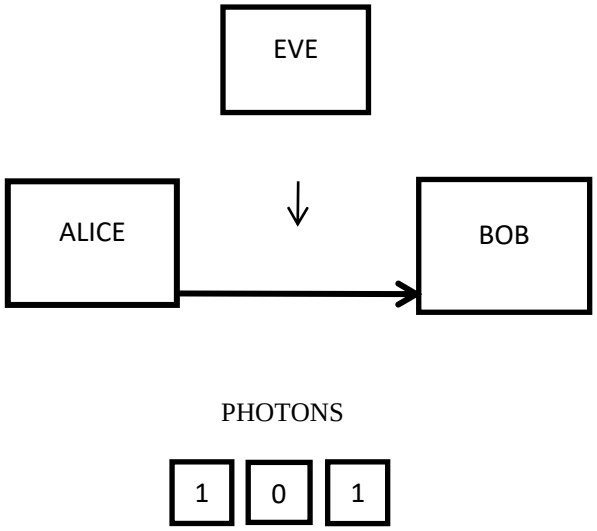

Figure 1: Encryption by Photons

Both errors and potential information leakage are removed during subsequent error correction and privacy amplification post-processing steps, leaving Bob and Alice with a shared key known only to them. Eavesdropper (Eve) is one who is trying to acquire data between the transaction, normally called as Eve[5]. Alice have only half set of time to read the data and other half for to access random value. If in case Eve interfere in transaction, shifting process will get discarded thus wont use that bit for their key. However if Eve try's to regenerate the photon that is demolished but as per quantum physics there is no way to read values of both side. So Security threat is minimized.

III. PROPOSED WORK

Figure 2 indicates how encryption works with QKD. We are using individual photons for transfer of encrypted key data between the person.The value of the bit either 1 or 0 is determined by photon itself. At the senders point a photon of series bits generated. The polarization of those photons is calculated at the receiver end. If a third person tries to intercept the data between transmission, the cryptographic file gets destroyed and send back to the sender itself.As we know that QKD works on uncertainty principle of quantum physics which makes impossible for the third person to determine the characteristic of the bit to be transmitted.So it will be impossible for him to send a duplicate file to receiver.If so the receiver end will identify that the number of bits transmitted is varied with the constant one so that receiver will get alert and end the transmission program.To determine the possibility of error we consider the number of bits to the receiver and sender.Comparison process removes the photon which is responsible for creating a private key.If session is secure cryptographic will be produced and it will be enabled for transmitting files securely.The technique of data transmission using photon to generate secure key is only a part of data encryption not all because of QKD.QKD allows us to access exchange data as physics law guaranteed.The generated key is totally secured and cannot be overwritten with high level of security. It has real time application like BB84 protocol and SARG protocol.

A. Encryption Approach

Basic approach of encryption is dealed here.As we know that it involves to blocks ,one is to convert the raw data to cypertext and to reconvert the cypertext into data. During this process to receive the data from the receiver a private key is necessary to view the data that is added between the transition. Normally a private key is one which

is used to access the data and also to convert the data. The encryption key is may be identical or there may be simple transform between the conversions. The key developed key is used to maintain the private information. Basic concept of QKD encryption is shown in the figure 2.

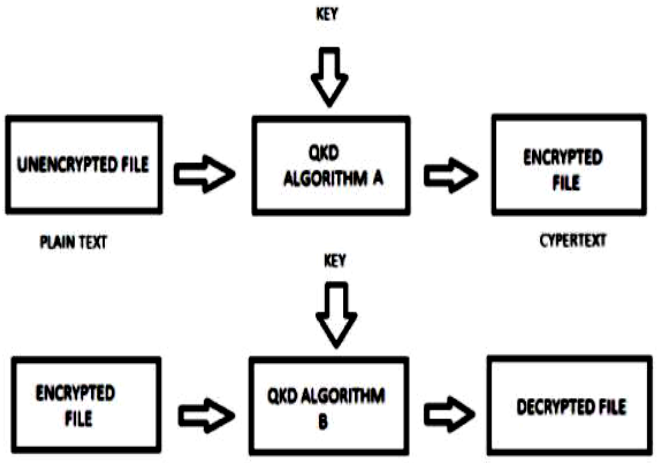

Figure 2: Basic Concept of QKD Encryption

B. Attaching Information Bit on the Photon – Key Exchange

Key exchange phase is also known as Raw key exchanging which promotes need for key shifting technique in future . First process involves sending secret key for initial authentication[6]. As said protocols like BB84 and SARG will be able to transmit bit values across quantum channel for different encoding states. The first process is to apply polarization on photons. If the system is compatible with integer it can be promoted into integer. The first person send a

ISSN No: - 2456 – 2165

key but its a start for key generation,it will be transform form first group of bits to the originally generated and protected key.

C. Reading Information Bits on the Receiver Side

In the above process photons with specified information is send to the receiver end. Next process involved is how actually quantum cryptography is gonna work in real time. While transmitting a data with vertical spin , the receiver too get the data with vertical filter. Thus they will successfully transfer bit of data using quantum substance. We use beam splitters to demonstrate one to many connection via optical network[7] It is important that receiver should use the correct filter to receive the original data. In this case transmitted data will be accompanied and dumped in phase shift keying or key verification.

D. Key Verification – Sifting Key Process

It is one of the mode where QKD and protocols like BB84 and SARG are made. In this method the outcome of that photon sent in vertical spin will get as in diagonal spin in receiver end. Key verification plays a vital role in this process.BB84 protocol will share the list of filters to the transmitter. Now they communicate to use different which filter to use for transition. Figure 3 shows the graph between key and eavesdrop ratio.

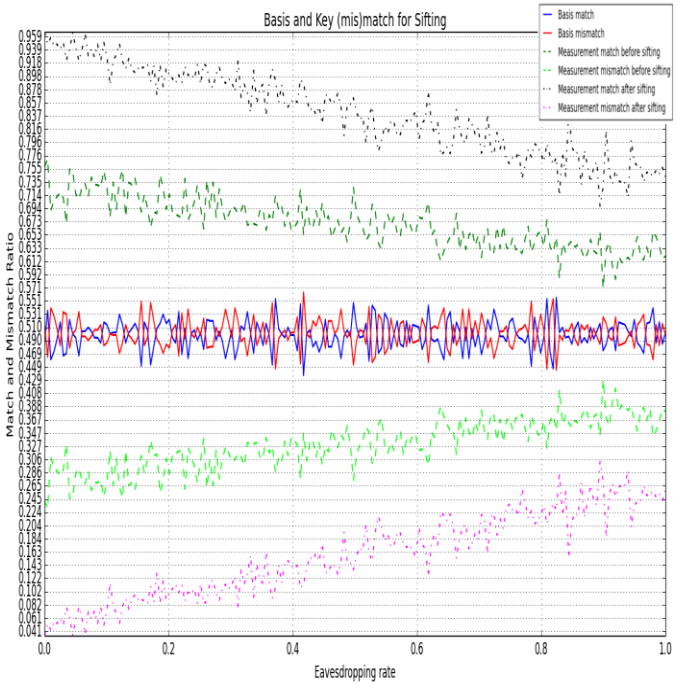

Figure 3: QKD Shifting Plot

In SARG protocol the receiver now send a list of output which is produced the first person Then need to use that list for sending to reduce the orientation of filter by the receiver. Now the first person opens for deduce the polarization. Sender and receiver discard all the cases then. In this method if we take BB84.

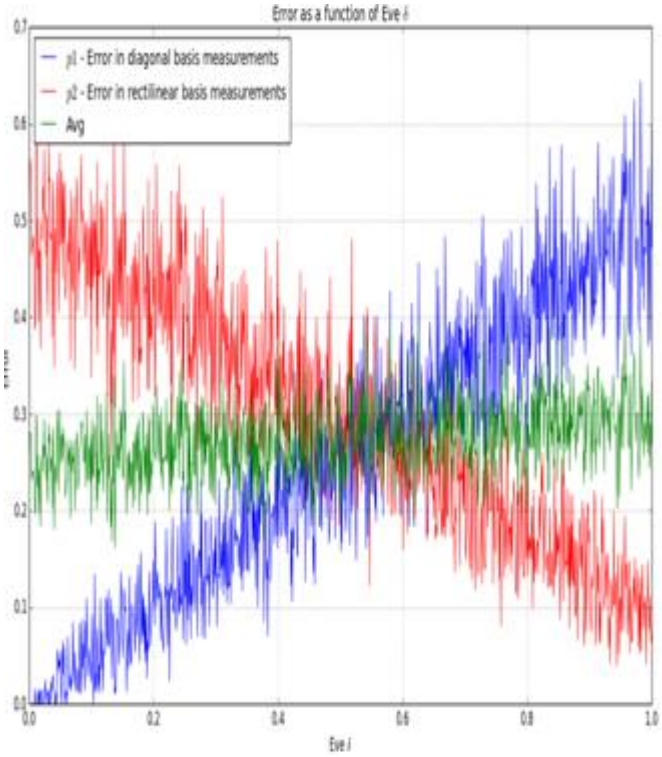

Figure 4: Biased error estimation

It is clear that communication between quantum channel and normal channel is applied by key verification. Figure 4 shows the biasing error estimation of signal which is transmitted. The two persons reading the data is done by bit by bit information. After shifting both ends will have a exact private key. Thus the key later shifting method will be of half of the real length.except those other bits are discarded in this process.

IV. CONCLUSION

In this paper, we have discussed about possibility and reliability of making QKD encryption in digital communication. It provides advanced data security which puts barrier for data theft between the data transit. As future relays on the hands of quantum computers, Security will be the major threat to those technologies. It is clear that only with the help of Quantum key distribution this shortcoming can be outlined. The proposed idea might have some problems in future but it can be overcome by further study in the encryption.

ISSN No: - 2456 – 2165

REFERENCE

[1]. K.G. Paterson, F. Piper, R. Schack, Why quantum cryptography?, Cryptology ePrint archive: report 2004/156, http://eprint.iacr.org/2004/156.
[2]. B. Schneier, Crypto-Gram: quantum cryptography, http://www.schneier.com/crypto-gram-0312.html#6, December 2003.
[3]. B. Schneier, Quantum cryptography: as awesome as It ispointless,Wired,http://www.wired.com/politics/security/commentary/securitymatters/2008/10/securitymatters_1016, October 2008.
[4]. C.H. Bennett, F. Bessette, G. Brassard, L. Salvail, J. Smolin, Experimental quantum cryptography, J. Cryptology 5 (1) (1992) 3–28; C.H. Bennett, G. Brassard, The dawn of a new era for quantum cryptography: the experimental prototype is working, Sigact News 20 (4) (1989) 78–82.
[5]. K.G. Paterson, F. Piper, R. Schack, Why quantum cryptography?, Cryptology ePrint archive: report 2004/156, http://eprint.iacr.org/2004/156.
[6]. P.D. Townsend, S.J.D. Phoenix, K.J. Blow, S.M. Barnett, Quantum cryptography for multi-user passive optical networks, Electron. Lett. 30 (1994) 1875–1877.