International Journal of Trend in Scientific Research and Development (IJTSRD)

International Open Access Journal

ISSN No: 2456 - 6470 | www.ijtsrd.com | Volume - 2 | Issue – 5

Digital Data Security by using Quantum Cryptography

Mohd. Amjad, Raju

Department of Computer Engineering, Faculty of Engineering

Jamia Millia Islamia, New Delhi, India

ABSTRACT

Security is the most common aspect of today's world, when all things are going to digitize then make them secure over the communication channel has become the prime aim of the digital service providers. Although many encryption and decryption techniques are available in the field of the cryptography, but they all are based on mathematical calculation which are difficult to solve but not impossible. The all existing techniques can be break by using quantum computer and some extra efforts. But Quantum Cryptography that is free from the mathematical calculations and large prime number factorization is solution of this type of problems. Quantum Cryptography based on the laws of physics and quantum mechanics which gives the most secure way of encryption and decryption. In this paper Key Generation and Exchanging of Key is implemented by using Visual Basic software to secure the digital data over the communication channel. Quantum cryptography will use Photons to transmit the information over the channel which are polarized at different orientation which are 00,450,900 and 1350 from sender at some basis and these polarized information is received by second party at other end and receiver will match the received photon with his photon on his basis and matched photons will form the Key, and if anyone try to hack that information both parties will come to know about the hacking.

Keywords: *Quantum Cryptography, Photon, Qubit, QKD, Basis.*

1. INTRODUCTION

Today we are shrinking because of internet and we are living in the Digital world in which all things whether our bank account, our credit/debit cards, PAN card, Driving License etc. all are going to be digitized. It means that we can access our data from any corner of our world. Internet has made our life very easy but with this easiness, it has also increase threat to our security. Today our all information is available on internet that ca be accessed by anyone from anywhere the world and miss used it. Hence it become for us that we provide security to our data when we digitized our data. And that security task can't be performed by a common person. Security task can be provided by the Security agencies. And from the ancient time people are aware toward the security of data, and for that purpose different Cryptography techniques are used to secure data. This project describes latest techniques of cryptography called Quantum Cryptography. But before that I would like to explain the basic concept of Cryptography

2. Importance of Quantum Cryptography

As we know security is the main concern of all the governments to make their digital data most secure so that no one can access that data without an authentication. Today most of the information of a person, organization, company and etc. are available on internet and anyone can access them and manipulate them to harm any person or organization. Hence each government are working on the security of the data. The cryptography techniques which are using to secure the data are good but not the best to secure the data, the all existing techniques of cryptography are based on mathematical calculation or on the large prime factorization of a number that is very difficult to break till know but after sometime it will be possible to break them by applying some extra effort or time on quantum computer at that time all existing techniques will be useless at that time we need such a technique which is free from mathematical calculation so that no one can hack it or break it. Quantum cryptography is the best of securing digital data over communication channel that based on physics principle and laws instead of mathematics. Since RSA encryption which is considered as the most secure technique of encryption which is based on large prime number is cracked many types by quantum computers to decode the code, hence it is compulsory that quantum encryption schemes must be developed to replace these techniques.

Quantum Cryptography is also capable of informing about the involvement of the third party if third party is trying to decode or hack our data.

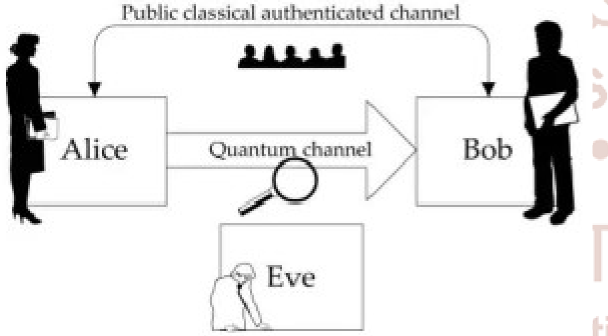


Figure 2.1: Communication by using Quantum Channel

The above diagram shows that two parsons common known as Alice and Bob are communicating with each other. On classical authenticated channel, It is possible that Eve (Third un-authorised person or hacker) can read copy that data and then send the original data to Bob without any tempering of data and none of them would be aware about the presence of Eve in between them. But,

If both Alice and Bob are communicating with each other by quantum cryptography channel, then it is not possible for Eve to hack that data. Because the characteristic of quantum mechanics that is No-cloning theorem, does not allow the exact copy of data. It means if Eve try to steal the data then it presence can be identified by the Bob because Eve broadcast the new message which will not match with Bob. Hence Quantum Cryptography is the best among all known cryptography techniques.

3. Elements of Quantum Cryptography

Following are the key elements of quantum cryptography

1. Photon: Light wave generated by LED at different orientation
2. Spin : angular momentum of photon in different direction
3. Polarization: spin of photon generates polarization.
4. Polarization Filter :A photon may or may not pass through a polarization filter to check this we have to mput a polarization filter in the way of photon

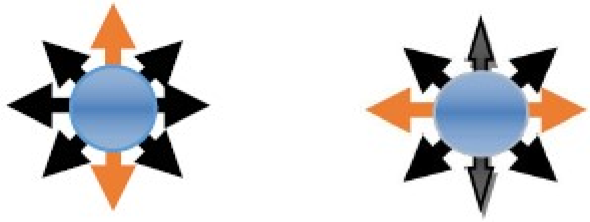


Figure 3.1: Rectilinear Polarization Mode

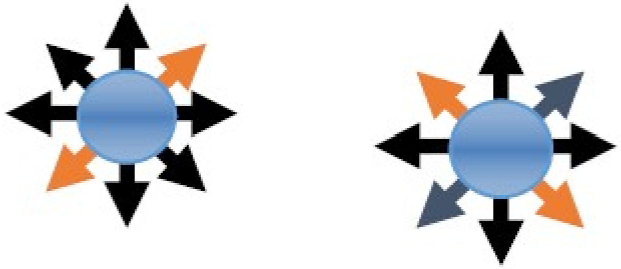


Figure3.2: Diagonal Polarization Mode

4. Quantum Superposition

Quantum Superposition is the main principle of quantum mechanics that is used to sum more than two quantum states to get new quantum state which is valid.

For example, Consider two quantum states |0> and |1>, now the quantum system will exist for all quantum states for by linear superposition of these two states.

Basic operation to get new states from existing states are shown blow

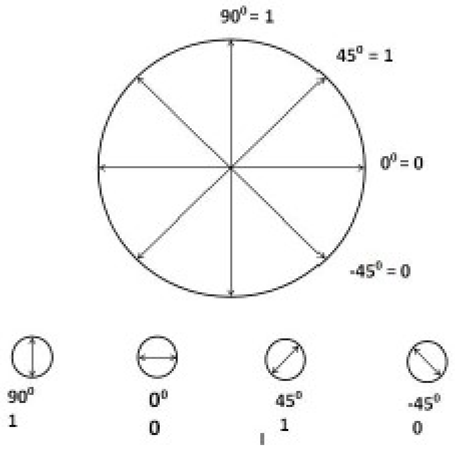


Figure 4.1: Polarization of photon

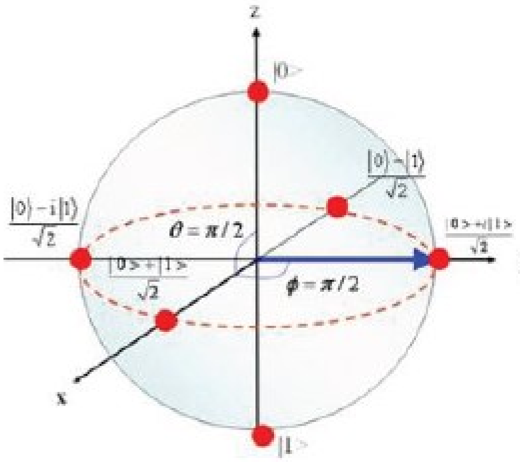

z
|0>
$\frac{|0\rangle-|1\rangle}{\sqrt{2}}$
$\frac{|0\rangle-i|1\rangle}{\sqrt{2}}$
$\theta=\pi/2$
$\frac{|0>+i|1>}{\sqrt{2}}$
y
$\frac{|0>+|1>}{\sqrt{2}}$
$\phi=\pi/2$
x
|1>

Figure 4.2: Geometrical Representation of Quantum states

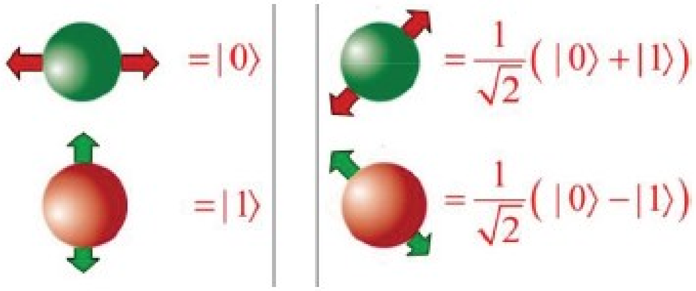

$=|0\rangle$
$=|1\rangle$
$=\frac{1}{\sqrt{2}}(|0\rangle+|1\rangle)$
$=\frac{1}{\sqrt{2}}(|0\rangle-|1\rangle)$

Figure 4.3: Photon polarization as qubit

1. Phase Gate

$$|0> \Rightarrow |0>$$
$$|1> \Rightarrow e^{i\phi}|1>$$
$$\alpha|0> +\beta|1> \Rightarrow \alpha|0> +e^{i\phi}\beta|1>$$

2. NOT operation

$$|0> \Rightarrow |1>$$
$$|1> \Rightarrow |0>$$
$$\alpha|0> +\beta|1> \Rightarrow \alpha|1> +\beta|0>$$

3. $\sqrt{NOT}$ Operation

$$|0> \Rightarrow \frac{1}{\sqrt{2}}(|0>+|1>)$$
$$|1> \Rightarrow \frac{1}{\sqrt{2}}(-|0>+|1>)$$

And all operation is must performed on superposition states.

5. Principle and Theorem

Quantum Cryptography is the techniques that are based on physics laws and principle which ensure that this one is the best technique of Security among all existing techniques of Cryptography. The principle and theorem on which quantum cryptography depends are as follows

5.1 Heisenberg Uncertainty Principle:

The Heisenberg uncertainty is the most famous principle of physics that say that two things in the universe can't be measured simultaneously. It states that "*the position and momentum of a particle cannot be simultaneously measured with arbitrarily high precision. There is a minimum for the product of uncertainties of these two measurements:*"

$$\Delta p\Delta m < \frac{h}{2}$$

This principle help in identifying an unauthorized person or third party Eve, when he tries copy the message of sender. Then Eve is not able to copy the accurate pattern of photons, which make his presence visible to both the parties involve in communication.

5.2 Heisenberg Notation

Because of simplicity and more practicality of Dirac notation, it is used to describe the basis notation of quantum system instead of Heisenberg notation. Dirac Notation is more practical than Heisenberg notation for providing fact in quantum Computing. In this orthonormal quantum states can be expressed as follow:

$$|\uparrow\rangle = |0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$$
$$|\downarrow\rangle = |1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$$

5.2.1 Kronecker Product

Kronecker Product is the mathematical representation of the combination of qubits into muti-qubit system. For 2-qubit system states can be obtained as follows:

$$|00\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix} \otimes \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix} \quad |10\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix} \otimes \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \end{bmatrix}$$

$$|01\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix} \otimes \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \end{bmatrix} \quad |11\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix} \otimes \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \end{bmatrix}$$

5.3 No-Cloning Theorem

In 1982, No-Cloning Theorem was stated by Wootters, Zurek and Dieks. And as the name of theorem indicates that nothing can be exactly copy(clone). It means that same copy of a state cannot be created in quantum mechanics which ensure the security of digital data. The theorem based on the fact that all quantum operations must be unitary linear transformation on the state

Proof:
Assume that Y be a unitary operator for cloning

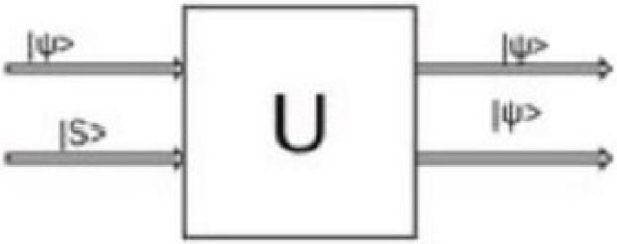


Figure 5.1: Cloning a quantum state

From the given diagram, we can say that

$$U|\psi>|S>=|\psi>|\psi> \quad \text{........ (1)}$$

For $\psi=\varphi$

$$U|\varphi>|S>=|\varphi>|\varphi> \quad \text{......... (2)}$$

By taking Inner product of equation (1) and (2)

$$<|S<\psi|U^{+}U|\varphi>|S>=<\psi|<\psi||\varphi>|\varphi>$$

$$<|S<\psi||\varphi>|S>=<\psi|<\psi||\varphi>|\varphi> \quad [U^{+}U=I]$$

$$<\psi||\varphi><S|S>=<\psi|\varphi><\psi|\varphi>$$

$$<\psi|\varphi>=<\psi|\varphi>^{2} \qquad [<S|S=1]$$

Let $<\psi|\varphi>=y$

Then ,

$$y=y^{2}$$

$$y-y^{2}=0$$

$$y(1-y)=0$$

$$y=0\ or\ 1$$

By the value of y that are 0 or 1, it proves that can be 0 or 1. It means and are either orthogonal or is in the same state. Hence it is proved that it is not possible to copy to quantum states exactly.

5.4 Fundamental of Quantum Key Distribution (QKD)

Quantum Key distribution is a way of key exchanging and key generating over an insecure communication channel. QKD, basically consists two classical users who most famous in the field of cryptography Alice and Bob, who are connected with each other through a communication channel which is not much secure. But they both want to communicate with each other securely with disclosing their important detail with any third person say Eve. In QKD , a quantum channel is used for communication which is much much better and secure than classical channel. A basic mode of QKD is shown in figure 1.

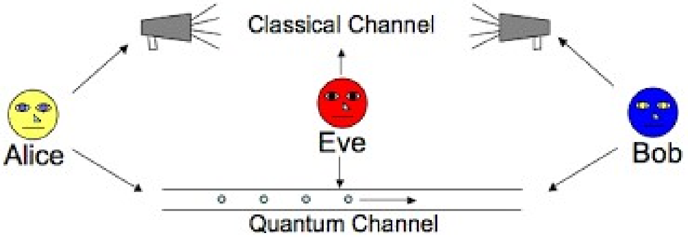


Figure 5.2: Basic Model of QKD

In the above figure, it is shown that an authorized person Eve trying to hack the data or information that is shared by Alice to Bob or Bob to Alice. But since the data is transmitted through quantum channel. Hence it is not possible for Eve to steal data, because he can guess the basis decided by Alice and Bob.

Generally following 8 steps are followed in QKD protocol.

1. Sender chooses Random number
2. transmits number over Quantum channel for communication
3. Choose the Sifting of photons
4. Reconciliation
5. Check involvement of third party if trying to hack data
6. if there is third party then amplify the Privacy
7. communication between sender and receiver
8. Finally key confirmation.

Suppose, first of Alice generates random numbers with the help of software or hardware random number generator. After choosing random number, he will use a specified Quantum Key Distribution protocol to convert or encode random numbers into quantum states that will be a sequence of signals from Alice's quantum light generator and transmit them over a quantum channel so that these quantum bits are received by Bob.

After receiving quantum states, Bob will apply his quantum measurement to each of received signal and covert that signal into a bit value.

After converting signal into bit, Bob will communicate with Alice over classical channel and inform him about the time slot when he received or detected the photons but he will not share the information about the bit values that is assigned by him to received photons. The bit stream which is obtained by Bob corresponding to the signal send by Alice is called *raw key*

After creating raw key, Bob and Alice select a random portion of their keys by public discussion and these keys are called *sifted keys*. Practically shifts keys of Alice and Bob are not correlated, but in ideal system there would be some correlation between the shift keys of both. There are some factors that create some transmission errors which arise due to background photons, noise detector and polarization imperfection.

After reading few literatures, it was concluded the typical error rate 1-5% is presented in the system and these errors most be located a corrected. By using error correction method over communication channel through which they are communicating with each other Bob reconciles his shifted key with Alice during this process parity information about shifted key is leaked. After this their keys will be partially secret now. After finding lots of errors in shift Key of Bob, they can find out an upper bound on any partially data that might be hacked by Eve through Alice's transmission of information in form of bit string. Quantum mechanics ensure that if Eve trying to measure the data, then a disturbance will be introduce in shift key of Bob that is strongly correlated to the partial information of Eve.

Like this on involvement of Eve a disturbance will be introduced to Bob shifted key which make alert to Bob, and after that Alice and Bob take out their reconciled keys a shorter, find bit string on which Eve's expected information is much less than one bit after an information-theoretic procedure known as *privacy amplification*.

In this procedure they use further public communications to agree to hash their reconciled keys into shorter final secret keys. For example, if Alice and Bob have 6 reconciled bits and their bound on Eve's information tells them that at most she knows 3 of these bits, they can agree to form two secret bits by XO Ring together the first 4 bits and the final 4 bits. Eve would have to guess at least one of the bits being XO Red in each case and so would be ignorant of the outcome. These two bits are therefore suitable for use in a cryptographic key. More generally, Alice and Bob can form their final secret bits from the parities of random subsets of their reconciled bits

5.5 BB84 Protocol

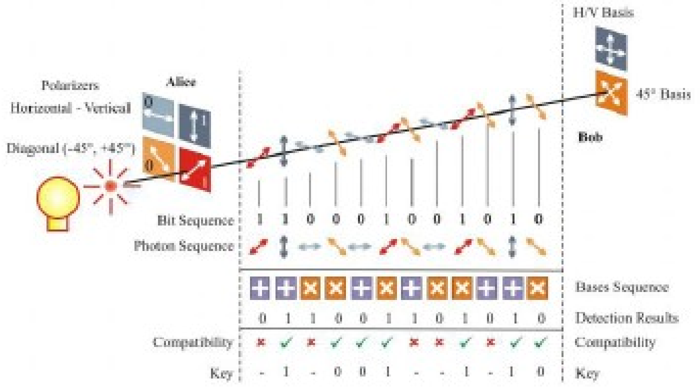


Figure 5.3:Quantum key Distribution Process

In 1984, a big change came in the field of cryptography, when two scientists Bennett and Brassard developed a new way of cryptography based on quantum mechanics which is called quantum cryptography. It was the first successful step in the field of quantum cryptography. This protocol was based on the quantum property that says information gain is not possible without disturbing the signal. This protocol was described as the secure exchange of private keys between sender and receiver with one time pad encryption.

BB84 protocol is a protocol that is based on the 'uncertainty principle' which says that quantum information cannot be copied or measured without disturbing the signal. This is the first protocol that gives intimation about the third person immediately, if he is trying to alter the data or have some partial data. This is very helpful to remove the 'eavesdropping' problem of cryptography.

In BB84, a stream of random numbers is generated by Alice and encodes them using the basis given in the figure 2. Alice selects this basis randomly and transmit the polarized information through quantum channel to Bob.

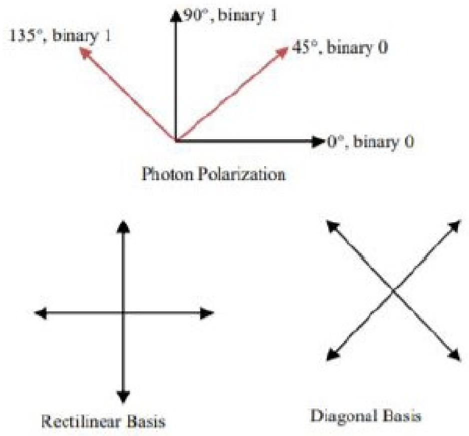
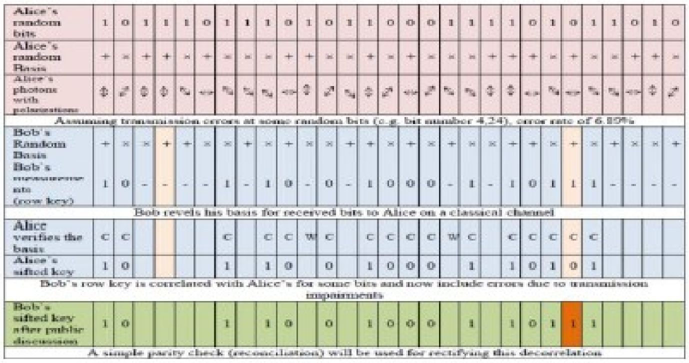


Figure 5.4: BB84 Coding

After transmitting photons by Alice, Bob gets them and choose a random basis for each bit. Now chances of choosing same basis as Alice choose is 50% on average. It means there is very low chance of getting same basis as Alice chooses. In ideal case in which no eavesdropping and no transmission errors the quantum bit error of the transmission line is less than 50%. But involvement of Eave increases this up to 75%. The following table shows this,

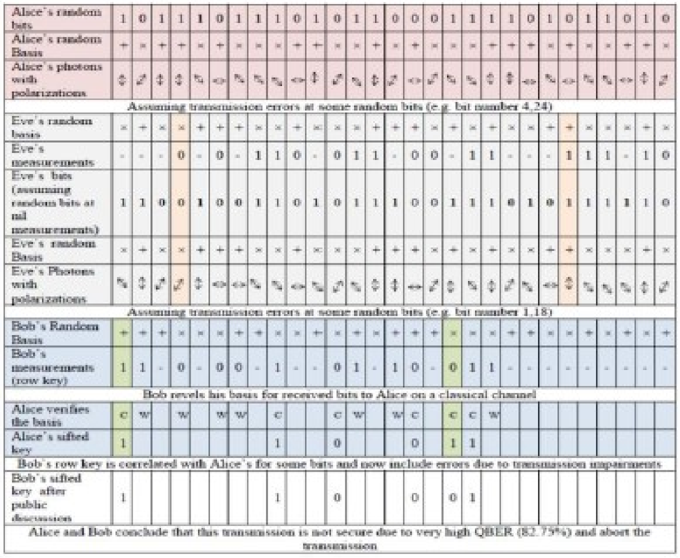


Alice's random bits	1	0	1	1	1	0	1	1	1	0	1	0	1	1	0	0	0	1	1	1	1	0	1	0	1	1	0	1	0
Alice's random Basis	+	×	+	+	×	+	×	×	×	+	+	×	×	+	×	+	×	×	×	+	+	+	×	+	×	×	+	+	×
Alice's photons with polarizations	↕	⤢	↕	↕	⤡	↔	⤡	⤡	⤡	↔	↕	⤢	⤡	↕	⤢	↔	⤢	⤡	⤡	↕	↕	↔	⤡	↔	⤡	⤡	↔	↕	⤢
Assuming transmission errors at some random bits (e.g. bit number 4,24), error rate of 6.89%																													
Bob's Random Basis	+	×	×	+	+	×	×	+	×	+	×	×	+	+	×	+	×	+	×	×	+	+	×	+	×	+	×	×	+
Bob's measurements (row key)	1	0	-	-	-	-	1	-	1	0	-	0	-	1	0	0	0	-	1	-	1	0	1	1	1	-	-	-	-
Bob revels his basis for received bits to Alice on a classical channel																													
Alice verifies the basis	C	C					C		C	C	W	C		C	C	C	C	W	C		C	C	C	C	C				
Alice's sifted key	1	0					1		1	0		0		1	0	0	0		1		1	0	1	0	1				
Bob's row key is correlated with Alice's for some bits and now include errors due to transmission impairments																													
Bob's sifted key after public discussion	1	0					1		1	0		0		1	0	0	0		1		1	0	1	1	1				
A simple parity check (reconciliation) will be used for rectifying this decorrelation																													

Table 5.1: BB84 protocol free from eavesdropping

From the Table 2, we come on conclusion that the Qubit Error Rate (QBER) is not more that 50% that is acceptable. After getting this result, Alice and Bob now decide to communicate continuously. Due to transmission error that is calculated less than 50%, the shifts keys of Alice and Bob are partially correlated. The errors present in transmission can be rectified by the reconciliation process of parity check.

In table 2 the involvement of Eave was shown with transmission error. After introducing Eave in the communication channel the QBER is increased very high that is greater than 50%. As both parties get this information, they would stop the communication.



Alice's random bits	1	0	1	1	1	0	1	1	1	0	1	0	1	1	0	0	0	1	1	1	1	0	1	0	1	1	0	1	0
Alice's random Basis	+	×	+	+	×	+	×	×	×	+	+	×	×	+	×	+	×	×	×	+	+	+	×	+	×	×	+	+	×
Alice's photons with polarizations	↕	⤢	↕	↕	⤡	↔	⤡	⤡	⤡	↔	↕	⤢	⤡	↕	⤢	↔	⤢	⤡	⤡	↕	↕	↔	⤡	↔	⤡	⤡	↔	↕	⤢
Assuming transmission errors at some random bits (e.g. bit number 4,24)																													
Eve's random basis	×	+	×	×	+	+	+	×	×	+	×	×	×	+	+	+	×	+	×	+	×	×	+	+	×	×	×	+	×
Eve's measurements	-	-	-	0	-	0	-	1	1	0	-	0	1	1	-	0	0	-	1	1	-	-	-	1	1	1	-	1	0
Eve's bits (assuming random bits at nil measurements)	1	1	0	0	1	0	0	1	1	0	1	0	1	1	1	0	0	1	1	1	0	1	0	1	1	1	1	1	0
Eve's random Basis	×	+	×	×	+	+	+	×	×	+	×	×	×	+	+	+	×	+	×	+	×	×	+	+	×	×	×	+	×
Eve's Photons with polarizations	⤡	↕	⤢	⤢	↕	↔	↔	⤡	⤡	↔	⤡	⤢	⤡	↕	↕	↔	⤢	↕	⤡	↕	⤢	⤡	↔	↕	⤡	⤡	⤡	↕	⤢
Assuming transmission errors at some random bits (e.g. bit number 1,18)																													
Bob's Random Basis	+	+	+	×	×	×	+	+	×	×	+	×	+	×	+	+	+	×	×	×	+	+	×	×	+	×	+	×	+
Bob's measurements (row key)	1	1	-	0	-	0	0	-	1	-	-	0	1	-	1	0	-	0	1	1	-	-	-	-	-	-	-	-	-
Bob revels his basis for received bits to Alice on a classical channel																													
Alice verifies the basis	c	w		w		w	w		c			c	w		w	c		c	c	w									
Alice's sifted key	1								1			0				0		1	1										
Bob's row key is correlated with Alice's for some bits and now include errors due to transmission impairments																													
Bob's sifted key after public discussion	1								1			0				0		0	1										
Alice and Bob conclude that this transmission is not secure due to very high QBER (82.75%) and abort the transmission																													

Table 5.2. BB84 protocol with Transmission Error and eavesdropping

5.6 Hacker Detection or Eavesdropper

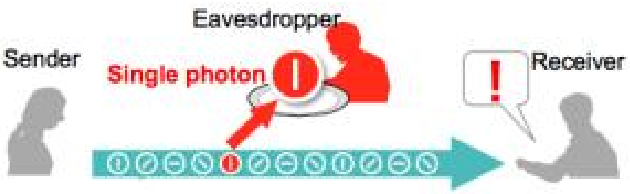


Figure 5.5: Hacker tries to hack data

Hacker detection or third party involvement reorganization is the main task of quantum cryptography. In quantum cryptography, if Sender (Alice) is sending some information to the receiver (Bob) in form of photon, and Eave is trying to hacker their information from the communication channel. Then this task will become very difficult for Eave. Only 50% chance will be met with their requirement because she does not know the basis of Sender (Alice) or receiver (Bob). So her involvement will be revealed in front of Alice and Bob. And they become alert toward the security of data.

6. Proposed Algorithm, Flow Chart and Work

Quantum Key Distribution is basically process of Key Exchange and Key Generation. Here I am given algorithm for Key exchange and Key generation process. To explain this process I am using the well known name in field of Cryptography that is Alice and Bob.

6.1 Algorithm (Alice)

1. Generate bit string
2. Choose random basis from rectilinear (+) and diagonal (×) to encode her bit string.
3. Choose photon(quantum state) for each bit
4. Transmit photon over communication channel at different polarization(
5. Record State, Basis and time of each photon
6. Repeat the process for random bit state

6.2 Algorithm (Bob)

1. Received transmitted photons by Alice
2. Choose random basis from rectilinear (+) and diagonal (×)
3. Record the Time, Basis and result
4. Communicate with Alice to know her basis
5. Match basis with Alice basis
6. Discard miss-matched photon and Alice will also do same
7. Matched bit will form Key

In above described algorithm Key generated by exchanging of photons between Alice and Bob. Which is the most secure key because no any mathematical work is done to generate this key, this key is generated only by using quantum physics.

6.3 Flow Chart

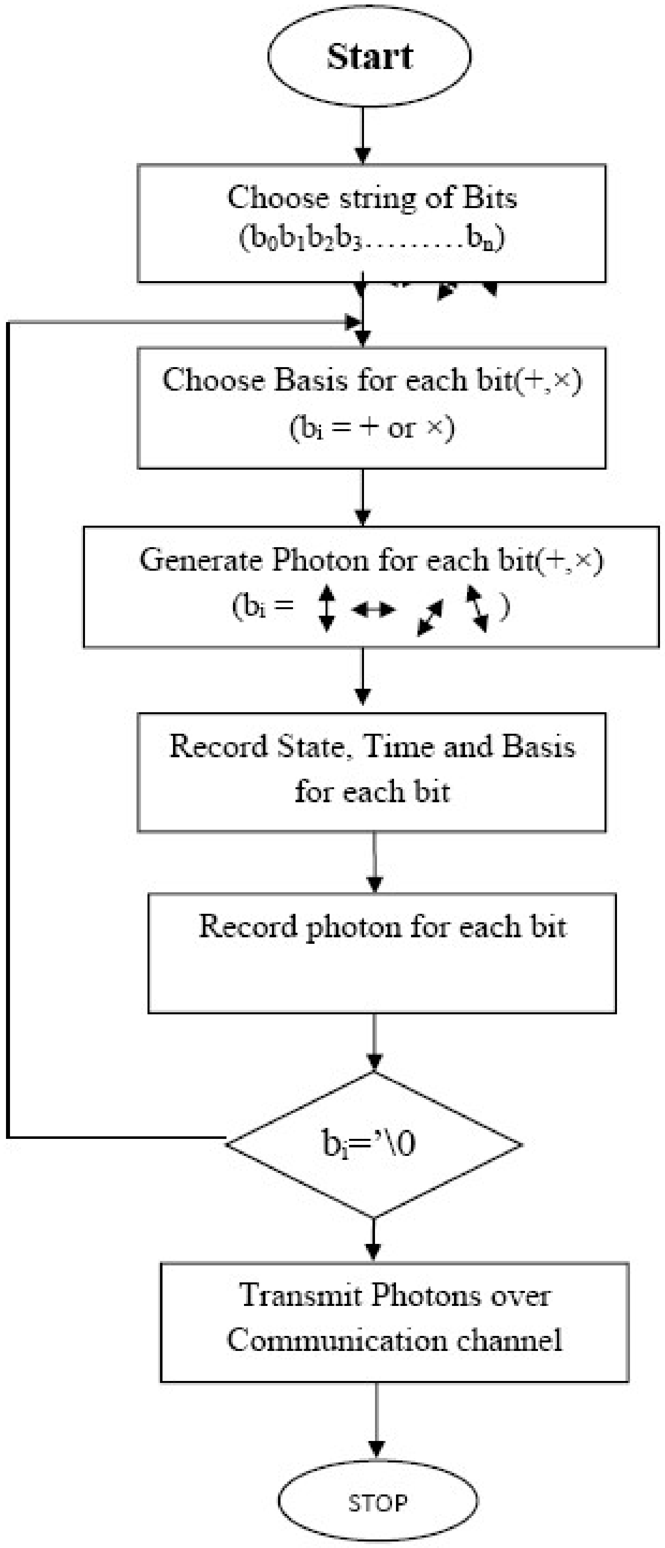

Start
Choose string of Bits
(b0b1b2b3.........bn)
Choose Basis for each bit(+,×)
(bi = + or ×)
Generate Photon for each bit(+,×)
(bi =)
Record State, Time and Basis for each bit
Record photon for each bit
bi='\0
Transmit Photons over Communication channel
STOP

Figure 6.1: Flow chart for transmission of Photons

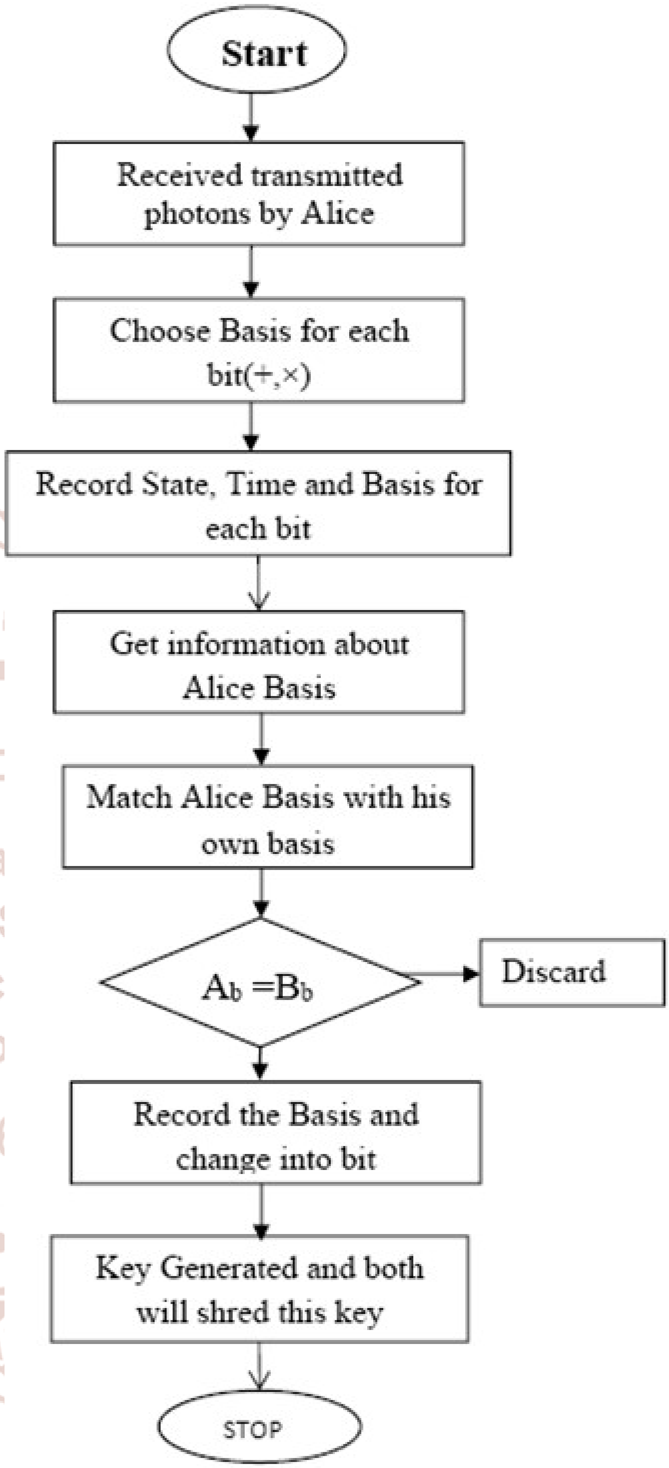

Start
Received transmitted photons by Alice
Choose Basis for each bit(+,×)
Record State, Time and Basis for each bit
Get information about Alice Basis
Match Alice Basis with his own basis
Ab =Bb
Discard
Record the Basis and change into bit
Key Generated and both will shred this key
STOP

Figure 6.1: Flow chart for key generation

7. Conclusion and Future Scope

After completing this project report, I come on conclusion that Quantum cryptography is the best of Key generation and Key Exchange between Sender and Receiver. All cryptography techniques which in use today are good, but in future all these techniques will be useless except few. This is the only cryptography techniques that are free from mathematical difficulty or we can say that it is not based on complex mathematical problem or on large prime factorizing problem. Quantum cryptography is the only one technique in the field of security that is using the laws of physics which make our digital data security much more secure. Since, it transmits the information in the form of quantum bits instead of bits as in classical cryptography. Photon which are transmitted with two basis that Rectilinear and Diagonal make the message more secure because if anybody tries to hack or steal data then his presence can be visible to both sender and receiver. This is the most special feature of quantum cryptography that it makes the Eavesdropper presence visible. With all these advantages it is not possible to implement it at a very large scale in the world because it the costlier way of security and since it is in its early stage so it is not foolproof. So for practical implementation of quantum cryptography we have to wait for some more decades.

Quantum Cryptography is the future of digital security which is compulsory for the coming generation when brilliant minds will be capable of finding the solution of toughest problem of mathematics, which will break the all existing cryptography techniques which are based on mathematical difficulties like large prime factorization and discrete logarithm. At that time quantum cryptography will be useful, right now it cannot be implemented because of cost and lack of resource. The future development will focus on faster photon detectors which can detects the fast moving electrons easily which is not present today. To make quantum cryptography commercial a big practical system will be implemented by the government because it cannot be implemented or commercialized without the help of government.

To make quantum key distribution more reliable and commercial for today's telecommunications infrastructure is the ultimate goal of cryptographers and enhance the transmission distance and rate of key generation.

REFERENCES

1. Bennett, C. H., Brassard, G.: Quantum cryptography: public key distribution and coin tossing. In: Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing, p. 175 (1984)
2. Neha Chhabra," Secret Key Generation and Eavesdropping detection using Quantum Cryptography:", (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 3 (2) ,2012,3348 – 3354
3. Shemin P A, Prof. Vipinkumar K S," E–PAYMENT SYSTEM USING VISUAL AND QUANTUM CRYPTOGRAPHY", International Conference on Emerging Trends in Engineering, Science and Technology (ICETEST - 2015), 24 (2016) 1623 – 1628
4. D. Bruß and C. Macchiavello, "Optimal Eavesdropping in Cryptography with ThreeDimensional Quantum States," Phys. Rev. Lett. 88,127901 (2002).
5. Brassard, Gilles; Claude, Crépeau; Jozsa, Richard; Langlois, Denis (1993). A Quantum Bit Commitment Scheme Provably Unbreakable by both Parties. FOCS 1993. IEEE. pp. 362–371.
6. N. Gisin, G. Ribordy, W. Tittel, H. Zbinden "Quantum Cryptography", Rev. of Mod. Phys. 74, pp. 145 - 195 (March 2002)
7. D. Bruß and C. Macchiavello, "Optimal Eavesdropping in Cryptography with ThreeDimensional Quantum States," Phys. Rev. Lett. 88,127901 (2002).
8. D. Mayers, "Unconditional security in quantum cryptography," J. Assoc. Comp. Mach., vol. 48, pp. 351–406, 2001
9. S. Wiesner, "Conjugate coding," SIGACT News, vol. 15, no.1, pp. 78– 88, 1983.
10. Siavash Khodambashi, Ali Zakerolhosseini A Quantum Blind Signature Scheme for Electronic Payments The 22nd Iranian Conference on Electrical Engineering (ICEE 2014), May 20-22, 2014, Sahid Beheshti University
11. William A. Fedaka and Jeffrey J. Prentisb Department of Natural Sciences, University of Michigan Dearborn, Dearborn, Michigan 48128 The 1925 Born and Jordan paper On quantum mechanics",2009 American Association of Physics Teachers

Authors

Dr. Mohd Amjad, currently working as Associate Professor in Department of Computer Engineering, Faculty of Engineering Jamia Millia Islamia, New Delhi-110025

Mr. Raju, Pursuing M. Tech Computer Engineering from Department of Computer Engineering, Jamia Millia Islamia, New Delhi-110024.