ISSN 2278-3091

Volume 9, No.3, May - June 2020

International Journal of Advanced Trends in Computer Science and Engineering

Available Online at http://www.warse.org/IJATCSE/static/pdf/file/ijatcse212932020.pdf

https://doi.org/10.30534/ijatcse/2020/212932020

Quantum Key Distribution: A Safer Alternate To Asymmetric Key Exchange Policies

Sreeparna Chakrabarti[1], Dr. G N K Suresh Babu[2]

[1] Research Scholar, Department of MCA, Visvesvaraya Technological University, Belgaum

[1] Assistant Professor, Department of Computer Science, Kristu Jayanti College, Bengaluru

chakrabartisreeparna@gmail.com

[2] Professor, Department of ISE, Acharya Institute of Technology, Bengaluru

gnksureshbabu@gmail.com

ABSTRACT

The encryption process of Symmetric Key Cryptography is quicker as compared to Asymmetric Key Cryptography, but the key exchange process is a challenge. This paper focuses on Quantum Cryptography techniques for that purpose as traditional digital cryptography techniques are not safe. In "Quantum Key Exchange" Technique, "Heisenberg uncertainty principle" and "quantum no cloning theory" are used to resist attacks. The Quantum Key Exchange is demonstrated through BB84 algorithm and the result is analyzed. Discussion is made on the practical applications of the technique

Key words: Quantum Key Cryptography, Quantum Key Exchange, BB84, Qubit.

1. INTRODUCTION

Cryptography is the process or technique of securing the communication among several parties via some communication channel in the presence of a potential intruder.

Among the two known techniques of cryptography viz. “Symmetric Key Cryptography” and “Asymmetric Key Cryptography”, the former demands the same key to be present with both the transmitter and receiver which gives rise to a big problem of secure key exchange. Additionally, millions of institutions like banks, hospitals, insurance companies etc. want to keep their stored data private too, for which they use Symmetric Key Cryptography as it is simpler and faster. Hence, they too need to transfer the key securely.

Traditional way of transferring and securing the keys are not full proof however strong the algorithm might be. The existing cryptographic algorithms are established on the concept of finding out the factors of a very large integer.[5] An algorithm, which is proved to be secure enough today, can cease to be so tomorrow with the advent of stronger computational systems which may lead to the event of easily factorizing such numbers. RSA algorithm, which is a popular Asymmetric Key Algorithm, suffers from chances of attacks in the future like: factoring the key [9]. Even comparatively new and unique Cryptographic method like ScDs Pyramid [6] method needs the exchange of a common key which might be breakable in the future.

Hence, with the progress of processing power of the systems, the traditional key exchange algorithms cannot be labelled as "Unbreakable Forever". This gave way to "Quantum Cryptography" where concepts of Quantum Physics are utilized to get a strong key exchange system which doesn't compromise the secrecy. A subset of it is the “Quantum Key Distribution System” which ensures safe exchange of Symmetric Key between the dispatcher and the receiver.

2. QUANTUM CRYPTOGRAPHY

2.1 Basic Concept

In Classical Cryptography, bits(0 or 1) are used to encode the information, whereas in "Quantum Cryptography" (which is a subset of "Quantum Computing"), “quantum bits”(qubits) serve that purpose. A qubit is the lowest unit of quantum data like the two polarization states of a photon-horizontal and vertical. In classical system, 0 or 1 are the two possible states of a bit and the states cannot be combined. But in Quantum System, the qubit could be in a coherent superposition of both the possible states. Moreover, a qubit can hold more information than a bit. It has been proven that 2bits of data can be transferred via a single qubit using a process called "Superdense Coding".

"Quantum Physics" is an area which deals with the particles that build up matter and studies about their interactions. "Quantum Cryptography" is based on dual pillars of "Quantum Physics":

(i) The Heisenberg Uncertainty principle: "The momentum (p) and position (x) of a particle could not both be exactly

measured simultaneously"[1] which means that "it's impossible to measure something at the subatomic level without altering it."[3]
Quantum Cryptographic Systems exchange information via a stream of photons and if any intrusion happens, the intruder tries to measure the polarization of the photons to know the secret message. In the process, the photons are also altered as per the principle. The source and the receiver thus discards the communication.

(ii) The norm of photon polarization: ‘A discrete photon can either be in a state of right circular polarization or left spherical polarization, or a superposition of the two. Stated in a different manner, a photon can as well be thought to have horizontal or vertical linear polarization, or superimpositions of both.’[2]

The photons are polarized into different polarizations viz. right circular, left circular or a superposition of the two while transmitting. This polarization changes when the intruder tries to measure the polarization or tamper with the photons.

Cryptography can be used in:
(i) Key distribution of classical cryptographic systems
(ii) Quantum Bit Commitment.
(iii) Quantum Coin Tossing [8]

2.2. Practical Implementation in “Quantum Key Distribution”

The sender will send a stream of photons to the receiver emitted from a photon gun, polarized vertically, horizontally or diagonally in the opposite direction using a polarizer:

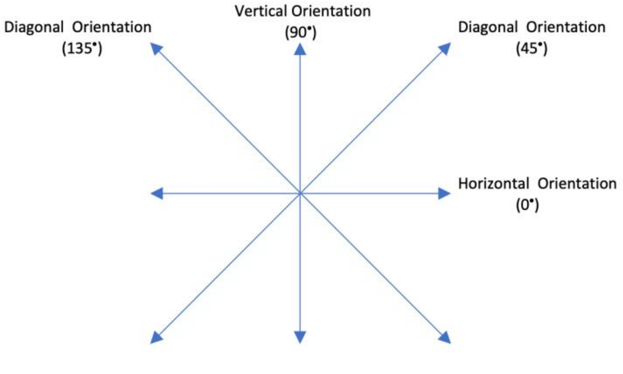

Figure 1: Orientations of polarized photons

The photons which reach the receiver will be filtered via a polarizer and measure the corresponding polarization which can be 0, 90, 45 or 135 degrees as presented in Figure 1. This is completed by picking a random base at the receiver's end. Now the receiver communicates to the sender about the respective bases chosen (in order) and based on that the sender says to the receiver which are the correct ones. In the process, the sender also understands which photons are to be kept to measure the final key.

But, the actual data received will never be communicated in this process. All the photons that could not be measured correctly by the receiver are then discarded. The remaining photons are then translated to 0 or 1 depending on their polarization value and the key is formed. This method is full proof because neither the sender not the receiver knows beforehand about the key.

3. QUANTUM KEY DISTRIBUTION

3.1 Basic Concept

The characteristics of Quantum Cryptography makes it suitable to be used for key exchange process in Symmetric Key Cryptography, this process is known as "Quantum Key Distribution" or in short QKD.

3.2 The Process

A diagrammatic step by step explanation of the whole process:
Step 1: Sender sends a random sequence of bits, converted to photons, which can be horizontal (↔), vertical (↕), left circular (⤢) or right circular (⤡). This conversion is done via an arbitrary base at the sender’s side, which can be either Rectilinear (R) or Diagonal (D).

Step 2: The receiver quantifies the polarization of the photons using a random sequence of bases, Rectilinear (R) or Diagonal (D). In the process some photons may be lost forever due to the choice of wrong base.

Step 3: The receiver records the resultant sequence of photon polarization values, also noting down which photons were lost (marked as cross in the table).

Step 4: The receiver uses a coding scheme to convert the polarization values to corresponding bits. The coding scheme followed:
(i)If the polarization values of the received photon is horizontal (↔) or left circular (⤢), the corresponding bit value is 0
(ii)If the polarization values of the received photon is vertical (↕) or right circular (⤡), the corresponding bit value is 1

Step 5: The receiver communicates the base values used by him to the sender as out of band data to make unquestionable that it differs from the actual message sent. Receiver then compares it with base he chose and communicates back the matching base values.

Step 6: Since both Sender and Receiver has the matching base values, which were chosen by both, the key value is formed by the bits corresponding to those base values.

3.3 Observations about QKD steps

Table 1: QKD Steps using an example value

Step 1								
Photon No.	1	2	3	4	5	6	7	8
Bits	0	1	0	1	1	1	0	1
Sender's Base	R	D	D	R	R	D	D	D
Polarization Values (Sender's side)	↔	⤡	⤢	↕	↕	⤡	⤢	⤡
Step 2&3								
Receiver's Base	R	D	R	D	R	D	R	D
Polarization Values (Receiver's side)	↔	×	↔	⤢	↕	⤡	×	⤡
Step 4								
Bits	0		0	0	1	1		1
Step 5								
Matching base	√				√	√		√

Table 1 shows an example of the process of QKD. Simulation tool has been used to replicate the whole communication process and actual results are being displayed here.

Few observations from Table 1:

(a)The polarization values of Step1 are not random, these experimental values are decided from the bits and corresponding base. Eg: the bit value for photon No.1 is 0. As per the coding scheme discussed above, 0 bit value means that the photon can be either horizontal (↔) or left circular (⤢). Since the sender's base is Rectilinear(R) i.e. either horizontal or vertical, the corresponding photon is horizontal (↔).

(b) Under Step 2&3, the polarization values (receiver's side) is decided by the polarization values of the photons sent by the Disseminator and the base choice of the receiver. It should be noted here that a base can have two possible orientations, namely Diagonal Base D can have two orientations: ⤢ and ⤡, whereas Rectilinear Base R can have two orientations: ↕ and ↔.

Few cases can arise:

Case 1: If the base chosen by the source and the receiver are the same and in the same orientation

In this case, the description of the classical polarized sinusoidal plane electromagnetic wave of the photon in the sender and the receiver's side will be identical. Like: in case of Photon1 in Table1, Rectilinear Base R is chosen in both the ends and the orientation is also the same. Hence, the polarization of the photon is horizontal (↔) in both sender and receiver sides.

Case 2: If the base chosen by the sender and the receiver are the same, but in different orientation

In this case, the photon will be destroyed at the receiver's end. Like: in case of Photon2 in Table1, Diagonal Base D is chosen in both sender's and receiver's side, but their orientations are not the same (one is at 45 degrees and the other is at 135 degrees). Hence the receiver could not measure the photon orientation and it is lost!

Case 3: If the base chosen by the despatcher and the receiver are not the same

In this case, the result is random and depends on the orientation of the bases on both the sides. But since the bases are different, anyways the value will be ignored.

3.3 Challenges

Practical systems up to 100km apart are using QKD based algorithms in many parts of Europe already. It has been thought that if the distance is more, a "Trusted Node"[4] can be incorporated to bridge the gap between the correspondent and the receiver nodes.

Moreover, Quantum Cryptographic Systems are very costly, hence they are only used for the highly confidential data. Before choosing between Classical and Quantum Cryptography, it is essential to calculate the cost of both and the loss in case data is lost.

Solution is to use hybrid methods:
(i) First Level-cost conscious classical methods
(ii) Second Level-Trusted Node Based QKD methods
(iii) Third level-Quantum Repeaters Based QKD method.

4. POSSIBILITY OF INTRUDER ATTACK IN QKD

4.1 Possibility of attacks

The cases which can occur if an intruder (Eve) wants to attack the communication channel during the transfer of photons are discussed below:

Case 1: If Eve tries to guess the communicated bits by trying to measure their polarization during transfer through the communication channel

Following "Heisenberg Uncertainty Principle", if Eve tries to measure the polarization value of a photon while transferring, the photon will be destroyed. Depending on the length of the symmetric key to be shared, the transmitter and the receiver has to decide the number of photons to be sent from the sender's side. If the receiver does not receive 25% of the sent photons, he can be sure of the existence of Eve or any other problem in the whole system. The key has to be discarded instantly in that case and Sender has to send the photon stream again.

Case 2: If Eve tries tampers with the sent photon and creates another photon and passes onto the Receiver

Though Eve tries to measure the orientation of the photon sent by the Sender, he will not be successful in approximately 75% of the times. Hence, when he creates another photon to send to the receiver, which mathematically will be incorrect 50% of the times. In that case Receiver will not receive 25% of the actual photons sent to him and he will guess the existence of Eve.

Case 3: If Eve tries to listen to the base of the Receiver when he tries to communicate the same to the sender

Eve cannot benefit in any way just by knowing the base because the actual photons are destroyed by then after measuring. Key value is measured by the polarization value of the photons, the base chosen, in no way, can reveal the actual key.

Case 4: If Eve tries to change the "base used by the Receiver" value when he tries to communicate the same to the sender

Eve can disturb the communication here once. If he changes actual base values while it was getting communicated between the sending side and receiving side parties, he can change the key values too. But as soon as Sender and Receiver starts to communicate the actual message, they will become aware that the key values they possess are not the same. But Eve cannot still know the actual key value.

4.2 Outcome

Hence, it is impossible for Eve to know the actual key value in any way. Practically, for extra safety, Sender and Receiver tests for the presence of Eve (in the Quantum Channel) by sharing some of the bit values from the ultimate outcome. Those bit values should be discarded from the key later. If the bits match, Eve is not present in the communication channel.

5. COMPARING QKD AND TRADITIONAL KEY EXCHANGE METHODS (TKEM)

5.1 Symmetric Key Confidentiality during exchange

TKEM: In Classical methods for Symmetric Key Algorithms, the Symmetric Key is exchanged using Asymmetric Key Algorithms. Constant research is needed to ensure the security of such algorithms. With the advent of powerful computing systems, the existing algorithms can never be considered as completely safe.

QKD: Quantum Cryptographic concepts are based on quantum physics theories which are constant and unbreakable. So, QKD is any day safer than the classical methods of symmetric key exchange.

5.2 Speed

TKEM: Depends on the internet speed.

QKD: As per the experiments conducted in “Europe's Cambridge Research Laboratory”, based on data logged for a month, average speed of QKD is around 10Mbps.

5.3 Distance

TKEM: Unlimited!

QKD: (i) Through wired communication channels, QKD can be applied over 2000km. An example is "The Beijing□Shanghai Backbone Network" in China. The project started in 2013 being carried out by "The National Development and Reform Commission of China" connecting Beijing, Shanghai, Jinan, Hefei and many other places.

(ii)Through wireless communication technologies, QKD can be executed up to 1200km. An example is the recent quantum communication among outer space and the ground parties via wireless passage by quantum communication satellite and stations present on the earth.

5.4 QKD is gaining popularity

QKD is gaining popularity amongst the Symmetric Key Algorithm Users. As the comparison suggests that related to the Traditional Key Exchange method it has an added advantage mainly due to the tight confidentiality properties. The companies which are already using QKD via optical fiber channels, have also setup a monitoring system for those. A wireless sensor network has the responsibility of taking care of the optical fiber lines which are susceptible to climate changes, wearing out with time, any vibrations etc.

6. APPLYING THE QKD TECHNIQUES IN REALITY

It all started with connecting two QKD appliances with an optical fiber. This idea works well for LAN/MAN. QKD could successfully be applied in any institute campus. A photon can travel a distance of around 100km. Currently, it has been prolonged to long distances, as discussed already, via intermediate nodes. These are called 'Trusted Nodes" which perform a phenomenon called "key hopping". In "key hopping", instead of direct transfer of information from sender to receiver, it travels via the nodes. So, the long distance QKD needed the use of new technologies where the transmissions are decrypted into classical bits at the Trusted Node and then they are encrypted again into qubits to transfer them ahead. But this technique needs complicated Key Management Schemes for node to node information travel.

According to reports, European optical fiber based “Quantum Key Distribution” Network (“Secure Communication Based On Quantum Cryptography” - SECOQC) was practically implemented in Tokyo and Vienna. In the above applications, other than key hopping technique, trusted transmits/relays were used for the purpose of connecting the Sender and Receiver. In such applications, both parties pooled a undisclosed key with the transmit relay in the middle and the relay makes the XOR end result of the 2keys public.[7]

Recently, systems have been implemented for free space QKD by implementing these "trusted nodes" in satellites.

7. VULNERABILITIES AND SOLUTIONS

In reality no perfect photon source is available with the current technology. Also, since these photon generators are bulky and expensive, lasers are used to generate qubits. These lasers form weak and phase randomized pulses where each pulse can have 2 or more photons in a pulse. These pulses become vulnerable to “Photon Number Splitting” or PNS attacks. In a PNS attack, Eve splits a single pulse with multiple photons into two pulses. Eve contains within himself one pulse while transmits the other to Receiver. Now, Sender and Receiver cannot be aware of Eve listening to the pulse in between and they won’t discard the key. So later Eve can get the key during the reconciliation process.

The most popular solution to the above attack till date is the use of decoy state method. In this method, besides the standard states, Sender should generate some decoy states to identify Eve. The difference between standard states and decoy states is in the intensity. Any attack on these decoy state would change the quantum bit error rate drastically notifying Alice and Bob of the presence of Eve in the channel. Researchers have also found vulnerabilities at the detection side like detector blinding attack. A widely used detector which uses Single Photon Avalanched Diode, the detector turns blind when the input photon intensity increases and generates output proportionate to the input power. In this case, Eve can manipulate the detector to generate linear output but first sending a strong optical power signal. Hence now Eve has total control of the detector and it sends signal based on her measurement which only gets detected at Bob’s end when their bases match. A viable solution can be MDI-QKD where secret keys are generated at time-reversed entanglement protocol. MDI-QKD not only secures the channel but also increases the reach long distance by resisting channel loss.

8. CONCLUSION

Continuous research is going on in the arena of quantum cryptography for the better practical implementation. The world is slowly turning “smart” and secure key transfer is a hot topic. Since Quantum Key Distribution also requires hardware updating for smooth running, it is a big challenge. QKD is very useful in government data exchange, medical data exchange, bank OTP exchange and many other security demanding systems.

The rise of Online Banking has also increased the vulnerabilities of such online transactions. The fraudsters are inventing new methods and techniques to break these transactions regularly [13]. This brings in security concerns to the customers and the banking systems. There has been numerous cases where banking systems of countries has failed because of such hacking practices. QKD and Quantum Cryptography are understandingly making so much buzz in the banking sector.

EHR(Electronic Health Record) is a digital variety of a patient’s therapeutic report. EHR has made big strides in the recently and the centralized data can be stored and transferred among different authorized organizations. This data can be the source for a very popular health tool for the future [11]. The transferred data should be kept confidential private and Quantum Cryptography and QKD can be the backbone for this network to maintain privacy of the data.

REFERENCES

1. Richard Beyler, **Werner Heisenberg**, *Encyclopedia Britannica*, last updated on 28th May 2020, available at https://www.britannica.com/biography/Werner-Heisenberg#ref524688.
2. **Wikipedia**, last updated on 24th May 2020, available at https://en.wikipedia.org/wiki/Photon_polarization.

3. Alex Hutchinson, **Lasers Could Send World's Most Secure Messages through Space**, *Popular Mechanics*, 26th August 2008, available at https://www.popularmechanics.com/space/satellites/a3597/4279669/
4. Don Hayford, **The Future of Security: Zeroing In On Un-Hackable Data with Quantum Key Distribution**, *Wired*, September 2014, available at https://www.wired.com/insights/2014/09/quantum-key-distribution/.
5. J Aditya, P.Shankar Rao, "**Quantum Cryptography**", *Proceedings of computer society of India*, 2005 available at https://cs.stanford.edu/people/adityaj/QuantumCryptography.pdf
6. Sreeparna Chakrabarti, Debabrata Samanta, **Image Steganography Using Priority-Based Neural Network and Pyramid**, *In: Shetty N., Prasad N., Nalini N. (eds) Emerging Research in Computing, Information, Communication and Applications*. Springer, Singapore, May 2016. https://doi.org/10.1007/978-981-10-0287-8_15
7. Qiang Zhang et al, **Large Scale Quantum Key Distribution: challenges and solutions,** *Optical Express*, Vol.26, No.18, September-2018. https://doi.org/10.1364/OE.26.024260
8. C. H. Bennett and G. Brassard, **Quantum cryptography: Public key distribution and coin tossing**, *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing*, volume 175, page 8. New York, 1984.
9. Sreeparna Chakrabarti, Dr.G.N.K.Suresh Babu, "**A Review On Encryption Algorithms For Secured Data Communication**", *IJRAR - International Journal of Research and Analytical Reviews (IJRAR)*, E-ISSN 2348-1269, P- ISSN 2349-5138, Volume.5, Issue 4, Page No pp.656-663, November 2018.
10. Navid Kagalwalla, Tanvi Garg , Prathamesh Churi , Ambika Pawar, "**A Survey on implementing privacy in Healthcare: An Indian Perspective**", *International Journal of Advanced Trends In Computer Science and Engineering (IJATCSE)*, ISSN 2278-3091, Volume 8, No. 3, May – June 2019. https://doi.org/10.30534/ijatcse/2019/97832019
11. Kanika, Jimmy Singla, "**Online Banking Fraud Detection System: A Review**", *International Journal of Advanced Trends In Computer Science and Engineering (IJATCSE)*, ISSN 2278-3091, Volume 8, No. 3, May – June 2019. https://doi.org/10.30534/ijatcse/2019/96832019