IJNRD.ORG ISSN : 2456-4184

International Research Journal IJNRD Research Through Innovation

INTERNATIONAL JOURNAL OF NOVEL RESEARCH AND DEVELOPMENT (IJNRD) | IJNRD.ORG

An International Open Access, Peer-reviewed, Refereed Journal

SECURE QUANTUM COMMUNICATIONS: USING QUANTUM PROPERTIES FOR SECURE DATA COMMUNICATION

Esha Jawaharlal

BTech in Computer Science and Engineering
Chengalpattu, India

Abstract : In today's world, communication has become an integral part in our day-to-day life. Computers are omnipresent. We are dependent on communication networks for almost everything from education to shopping. They are virtually found in every industry and households as everyone owns at least one mobile device. Our biggest threat is the vulnerability of the current digital communication methods. The real transformation and ease of communication in our society is the development of large-scale networks that can interlink multiple devices together. Due to this development, the way of communication over the decades has widely improved. However, most of these communications occurs insecure modes requiring various methods to protect the channels for communication. To attain a safe and secure communication method, we can utilise the idea of quantum mechanics for encrypting the data packets.

Keywords: **Cryptography, Data Packets, Probability, Quantum, Quantum Conjugate, Quantum Mechanics**

1. INTRODUCTION

Researchers are developing protocols for ultra-secure communication using the properties of quantum mechanics and the present global quantum networks that increase the power available in the quantum world. Cryptography protects the information passed during communication by providing the key components. Cryptography is the field of science filled with secrets, that allows various information to be shared between long distances. It secures the passwords and personal data from leakage.

Quantum communication is a field of applied quantum physics that closely relates to quantum teleportation and quantum information processing. The most interesting feature of quantum communication is the protection of information channels through quantum cryptography. Most modern cryptographical methods use factoring-based problems which are hard to solve using regular digital computers, hence the improvement and development of quantum computers will make us re-examine the method used to secure the data. The most developed application of quantum cryptography is the quantum key distribution (QKD). QKD describes the features and uses of quantum mechanics to perform information security and cryptographical tasks.

2. CLASSICAL SECURITY TECHNIQUES

2.1 Encryption

The most used technique that encodes the key making it hard for an unauthorised party to understand and decode. Since it is hard to decode, many communication methods use a weak encryption method. Many encryption techniques are subjected to man-in-the-middle attack. Classical encryption communication is protected from eavesdropping but does not provide authentication or anonymity.

2.2 Steganography

The method by which data can be hidden within other non-important data. Thus, a watermark proving ownership embedded in the data of a picture, in such a way it is hard to find or remove. For instance, incase of communication, telephone number can be hidden in an mp3 file, hence going unnoticeable.

An advantage of steganography is the deniability, unless provided with evidence of the presence of the data, one can deny that the file contains the data.

2.3 Identity based networks

Undesirable or malignant way of behaving is conceivable on the computerized networks since the web is totally mysterious. Identity based networks supplant the capacity to stay mysterious and are innately more dependable since the personality of the shipper and beneficiary are known.

2.4 Anonymised networks

As of late, unknown systems administration has been utilized to get correspondences. On a fundamental level, an enormous number of clients running a similar framework, can have correspondences directed between them so that it is extremely difficult to distinguish what the total message is, which client sent it, and where it is eventually coming from or going to.

3. QUANTUM COMMUNICATION

Compared to regular communication, quantum communication is comparatively more secure as they rely on photons which is the reason, they cannot be cracked but the cost of building one is high.

Light is comprised of a particle known as photons. Photons is a particle that serves as the quantum of electromagnetic field, including EM radiations such as light and waves. Photons have no weight or mass and move at the speed of light in vacuum, 3 m/s. According to Maxwell, photons are electric fields travelling through space. Whenever an electron falls from a higher orbit falls to a lower orbit, then a photon is formed.

3.1 HISTORY

Quantum Cryptography was first coined by Stephen Wiesner and Gilles Brassard. At around 1970s, Wiesner, a student at Columbia University introduced the idea of quantum conjugate coding. In the paper he published, he explained the way to store and transmit two messages by encoding them as two observables conjugate such as linear and circular polarised photons. When Charles H. Bennett and Gilles Brassard met at the 20th IEEE Symposium on the Foundations of Computer Science, that they found a way to incorporate Wiesner's theory and findings. The main discovery was when they realised photons were used to transmit the messages rather than to store them. In 1984, using their discovery Bennett and Brassard invented a secure mode of communication known as the BB84. After which it was followed by a proposal stated by David Deutsch who used non-locality and Bell's inequalities to achieve a secure key distribution. In 1991, Arthur Ekert explained the entanglement-based quantum key distribution in depth.

Kak's three-stage protocol proposed the random rotation polarisation. This method can be used for unbreakable encryption of data packets if single photons are used. This method utilises quantum mechanics entirely for cryptography whereas quantum key distribution uses some concepts of mathematical cryptography.

The BB84 method is the basis of quantum key distribution methods. Many companies such as Toshiba, SeQureNet and ID Quantique manufacture quantum cryptography systems.

3.2 BB84

A quantum-key distribution method entirely developed by Charles Bennett and Gilles Brassard. It was the first protocol developed. The protocol is secure and depends on two conditions:

- The quantum mechanics property that information gain during the signal distribution is only possible if one of the two states is non-orthogonal. (Non-cloning theorem)

  Non-cloning theorem states that:
  "It is impossible to create an independent and identical copy of an arbitrary unknown quantum state".
  This theorem has a time-reversal method and a non-deleting theorem. Hence together they point the interpretation of quantum mechanics. The non-cloning theorem focuses on the pure states.
- The presence of a public channel, authenticated.

It can be explained as a method used to securely communicate a private key from one system to another.

Description

Amelia wishes to send a private key to Bailey. She starts with two strings a and b each consisting of the length, n.
She encodes them as a tensor product of q orbits.

$$|\psi\rangle = \bigotimes_{i=1}^{n} |\psi_{a_i b_i}\rangle,$$

where ai and bi are the i-th bits of a and b.
Together, aibi give us an index into the following four qubit states:

$$|\psi_{00}\rangle = |0\rangle,$$
$$|\psi_{10}\rangle = |1\rangle,$$
$$|\psi_{01}\rangle = |+\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle,$$
$$|\psi_{11}\rangle = |-\rangle = \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle.$$

Amelia sends the message over a public and authenticated quantum channel E to Bailey. Bailey receives a state $\mathcal{E}(\rho) = \mathcal{E}(|\psi\rangle\langle\psi|),$, where E represents both the effects of noise in the channel and eavesdropping by a third party, Esther.
But since only Amelia knows the value of b, Bailey and Esther cannot easily distinguish the states of the qubits. Even after Bailey receives the value of b, Esther cannot find it due to the presence of non-cloning theory. The probability of Esther figuring out right using measurement that the bias is ½ of a particular qubit orbit.
Bailey then generates a random string of bits b' of the same length n and then calculates the qubit received from Amelia, a'. Bailey now publicly announces that he has received Amelia's transmission. Amelia then knows she can now safely announce b, i.e., the bases in which the qubits were prepared.
Bailey communicates over a public channel with Amelia to determine which b and b' are not equal. Both Amelia and Bailey now discard the bits in a and a' where b and b' do not match.
For the remaining k-bits where Amelia and Bailey measured the same bases, Amelia can randomly choose k/2 bits and announces her choice publicly. Both Amelia and Bailey announce these bits publicly and analyse to check if a certain number of them match. If this check passes, Amelia and Bailey proceed to use privacy amplification methods to create some number of shared secret keys. Else, they cancel and restart.

4. ADVANTAGES

Cryptography is the greatest and the strongest method available for securing data during communication. However, basic cryptography cannot ensure entire security for a long duration. For securing the data for a loner period of time, the concept of quantum cryptography can be used.
For example, assume the data security required in a bank. The typical cryptography method cannot provide security for more than 30 years but bank stakeholders would require security for a longer period with indefinite length.
Even healthcare industry, under the Health Insurance Portability and Accountability Act, medical records must be kept confidential. Paper documents get shredded after a period of time but digital documents leave a digital trace. The quantum cryptography method can secure digital data for over 100 years.
Quantum communication is also used in militaries and government, as government must keep the military documents confidential. Until now, the documents have been kept a secret for over 60 years.
With many previous theories and experiments, it is proven that quantum key distribution can travel through a noisy channel and still remain secure regardless of the distance. The communication through noisy channel can be reduced by using quantum repeaters. Quantum repeaters have the ability to resolve any kind of quantum communication error in an efficient way. Quantum repeaters, which are quantum computers, can be kept as segments over the noisy channel to ensure the security of communication. Quantum repeaters ensure this by purifying the segments of the channel before connecting them creating a secure line of communication. Sub-par quantum repeaters can provide an efficient amount of security through the noisy channel over a long distance.

5. APPLICATIONS

5.1 QUANTUM COIN FLIPPING

Quantum coin flipping protocol is used when the two participants communicating do not trust each other. The parties communicate through a quantum channel and exchange information through the transmission of qubits. But since, they do not trust each other, they expect the other to cheat. Hence, most effort is spent in ensuring both the parties receive equal amount of advantage to produce an outcome. The ability to influence the outcome is known as bias, this protocol aims in reducing the bias of the dishonest player.
Quantum communication protocols, including quantum coin flipping, have been displayed to give huge security benefits over traditional correspondence, however they might be viewed as challenging to acknowledge in the reasonable world.

A coin flip protocol generally occurs when:

- Amelia picks a basis (either rectilinear or inclining) and creates a series of photons to send to Bailey in that premise.
- Bailey haphazardly decides to gauge every photon in a rectilinear or diagonal basis, noticing which basis he utilized and the deliberate worth.
- Bailey freely surmises which basis Amelia used to send her qubits.
- Amelia declares the basis she utilized and sends her unique string to Bailey.
- Bailey affirms by contrasting Amelia's string with his table. It ought to be impeccably corresponded with the qualities Bailey estimated utilizing Amelia's basis and totally uncorrelated with the inverse.

Cheating happens when one player endeavours to impact, or increment the likelihood of a specific result.
One theoretically sure-fire way for Amelia to cheat is to utilize the Einstein-Podolsky-Rosen (EPR) paradox. Two photons in an EPR pair are anticorrelated; that is, they will generally be found to have inverse polarizations, given that they are estimated in a similar premise. Amelia could create a string of EPR matches, sending one photon for every pair to Bailey and storing the other for herself. At the point when Bailey expresses his speculation, she could gauge her EPR pair photons in the contrary premise and acquire an ideal connection to Bailey's contrary table.
Bailey could never realize she cheated. Nonetheless, this requires abilities that quantum technology as of now does not have, making it difficult to do. To effectively execute this, Amelia would should have the option to store every one of the photons for a lot of time as well as measure them with close to consummate proficiency. This is on the grounds that any photon lost away or in estimation would bring about an opening in her string that she would need to fill by speculating. The more theories she needs to make, the more she gambles with recognition by Bailey for cheating.

5.2 QUANTUM COMMITMENT

Like quantum coin flipping, this protocol is also used when two parties that do not trust each other are involved. A commitment scheme permits a party Amelia to fix a specific worth (to "submit") so that Amelia cannot change that worthwhile simultaneously guaranteeing that the beneficiary. Bailey cannot learn anything about that worth until Amelia uncovers it. Such responsibility plans are usually utilized in cryptographic conventions.

5.3 BOUNDED AND NOISY QUANTUM STORAGE MODEL

One chance to build genuinely secure quantum commitment and quantum oblivious transfer (OT) protocol is to utilize the bounded quantum storage model (BQSM). In this model, it is expected that how much quantum information that an enemy can store is restricted by some known steady Q. Be that as it may, no restriction is forced on how much traditional (i.e., non-quantum) information the enemy might store.

The idea is that protocol parties trade more than Q quantum bits (qubits to basic thought). Since even an exploitative party cannot store all that data (the quantum memory of the enemy is restricted to Q qubits), a huge piece of the information should be either estimated or disposed of. Compelling dishonest parties to quantify a huge piece of the information permits the convention to dodge the inconceivability result, responsibility and unmindful exchange conventions can now be carried out.

The advantage of the BQSM is that the presumption that the foe's quantum memory is restricted is very reasonable. With the present innovation, storing even a solitary qubit dependably throughout an adequately lengthy timespan is hard.

An extension of the BQSM is the noisy-storage model introduced by Wehner, Schaffner and Terhal. Rather than considering an upper bound on the actual size of the enemy's quantum memory, a foe is permitted to utilize imperfect quantum storage gadgets of varying size. The degree of defect is demonstrated by noisy quantum channels. For sufficiently high noise levels, similar natives as in the BQSM can be accomplished and the BQSM structures a unique instance of the noisy-storage model.

5.4 POSITION BASED QUANTUM CRYPTOGRAPHY

The aim of position-based quantum cryptography is to use the geographical location of a party as its only credential. For instance, one needs to send a message to a player at a particular location with the assurance that it must be perused assuming the receiving party is located at that specific position. In the essential task of position-check, a player, Amelia, needs to persuade the (genuine) verifiers that she is situated at a specific point.

5.5 DEVICE- INDEPENDENT QUANTUM CRYPTOGRAPHY

A quantum cryptographic protocol is device-independent in the event that its security does not depend on believing that the quantum gadgets utilised are honest. Accordingly, the security analysis of such a convention needs to think about situations of imperfect or even malicious gadgets.

Mayers and Yao proposed idea of designing quantum protocols utilizing "self-testing" quantum contraption, the interior tasks of which can be found by their in to out statistics. Then, Roger Colbeck in his Thesis proposed the utilization of Bell tests for really taking a look at the genuineness of the gadgets. From that point forward, a few issues have been displayed to concede genuine secure and gadget free conventions, in any event, when the real gadgets playing out the Bell test are significantly "noisy," i.e., a long way from being ideal.

6. IMPLEMENTATIONS

6.1 SINGLE PHOTON SOURCE ASSUMPTION

The hypothetical reason for quantum key distribution expects a single photon source. However, single-photon sources are challenging to build and most genuine quantum cryptography frameworks utilize faint laser sources as a mechanism for data move. These multi-photon sources open a pathway for eavesdropping attacks, especially a photon splitting assault. An eavesdropper, Eve, can part the multi-photon source and hold one duplicate for herself. Different photons are then communicated to Bailey with next to no estimation or follow that Eve caught a duplicate of the information. The researchers accept they can hold security with a multi-photon source by utilizing decoy states that test for the presence of an eavesdropper. However, in 2016, scientists fostered a close to consummate single photon source and gauge that one could be created sooner rather than later.

6.2 IDENTICAL DETECTOR EFFICIENCY ASSUMPTION

Practically speaking, multiple single-photon detectors are utilised in quantum key distributions gadgets, one for Amelia and one for Bailey. These photodetectors are tuned to distinguish an approaching photon during a short window of a couple of nanoseconds. Because of assembling contrasts between the two identifiers, their separate location windows will be moved by some limited amount. An eavesdropper, Eve, can exploit this finder shortcoming by estimating Amelia's qubit and sending a "phony state" to Bailey. Eve first catches the photon sent by Amelia and afterward produces one more photon to send to Bailey. Eve controls the stage and timing of the "faked" photon in a way that keeps Bailey from identifying the presence of a busybody. The best way to kill this weakness is to eliminate differences in photodetector productivity, which is challenging to do given limited assembling fault tolerance that cause optical way length contrasts, wire length contrasts, and other defects.

7. CONCLUSION

Quantum cryptography has been primarily related to the improvement of quantum key distribution protocols. Tragically, symmetric cryptosystems with keys that have been disseminated through quantum key circulation become wasteful for huge organizations (numerous clients), on account of the need for the foundation and the control of numerous pairwise secret keys (the alleged "key-administration issue"). In addition, this dispersion alone does not address numerous other cryptographic assignments and capacities, which are of indispensable significance in daily existence. Kak's three-stage protocol has been proposed as a strategy for secure correspondence that is completely quantum dissimilar to quantum key dispersion, in which the cryptographic change utilizes traditional calculations.

Quantum communication is hence a more secure way to communicate and transfer data through various channels.

8. REFERENCES

[1] M. A. Nielsen, and I. L. Chuang, “Quantum computation and quantum information,” (Cambridge University Press, Cambridge,2000).
[2] Holevo, “Quantum Systems, Channels, Information: A Mathematical Introduction,” (De Gruyter, BerlinBoston,2012).
[3] Bengtsson and K. Zyczkowski, “Geometry of quantum states: An Introduction to Quantum Entanglement,” (Cambridge University Press, Cambridge2006).
[4] M. Hayashi, “Quantum Information Theory: Mathematical Foundation,” (Springer- Verlag, Berlin,2017).
[5] https://en.wikipedia.org/wiki/Quantum_cryptography
[6] https://en.wikipedia.org/wiki/Secure_communication
[7] https://en.wikipedia.org/wiki/No-cloning_theorem