International Research Journal of Innovations in Engineering and Technology (IRJIET)

ISSN (online): 2581-3048

Volume 3, Issue 11, pp 73-76, November - 2019

Quantum Communications and Cryptography

[1]P. Sirsat, [2]A. Nalamwar

[1,2]MCA Student, Department of Research and PG Studies in Science & Management, Vidyabharti Mahavidyalaya, Amravati, India

Abstract - **Internet has become the most popular carrier of information exchange in every corner of our life, which is beneficial for our life in almost all aspects. With the continuous development of science and technology, especially the quantum computer, cyberspace security has become the most critical problem for the internet in near future. In this paper, we focus on analyzing characteristics of the quantum cryptography and exploring of the advantages of it in the future internet. It is wealth nothing that we analyze the quantum key distribution (QKD) protocol in the noise-free channel. Moreover, in order to simulate real situations in the future Internet, we also search the QKD protocol in the noisy channel. The results reflect the unconditional security of quantum cryptography hypothetically, which is suitable for the Internet as ever -increasing challenges are expectable in the future.**

Keywords: Quantum Cryptography; Security; Quantum; Quantum Key Distribution (QKD); Polarization; Encryption; Photons.

I. Introduction

In their formative 1984 paper, Bennett and Brassard argued that some basic laws of physics may prove useful in cryptographic tasks. They considered first the task of key distribution between distant partners and noticed that quantum signals are ideal trusted couriers: if the eavesdropper Eve tries to obtain some information, her action cannot remain concealed, because measurement modifies the state or, equivalently, because of the no-cloning theorem. In the second part of their paper, they turned to the task of bit-commitment and proposed a quantum solution relying on entanglement. In 1991, Ekert independently re-discovered quantum key distribution: his intuition was based on entanglement, more specifically on Bell's inequalities. These two works are the milestones of the field, even if precursors for these ideas had been brought up. The fact that security is based on physical laws leads to the hope that quantum cryptography may provide the highest possible level of security, namely security against an adversary with unrestricted computational power; in the jargon, unconditional security.

II. Overview of the Quantum Cryptography

"Cryptographies the process of encrypting data, or converting plain text into scrambled text so that only someone who has the right 'key' can read it"

In classical cryptography communicating parties need to share a secret sequence of random numbers, the key, that is exchanged by physical means and thus open to security loopholes. The classical cryptography does not detect eavesdropping like quantum cryptography, also with increase in computing power and new computational techniques are developed, the numerical keys will no longer be able to provide satisfactory levels of secure communications. These flaws led to the development of quantum cryptography; whose security basis is quantum mechanics.

"Quantum cryptography, also called quantum encryption, applies principles of quantum mechanics to encrypt messages in a way that it is never read by anyone outside of the intended recipient." It takes advantage of quantum's multiple states, coupled with its "no change theory," which means it cannot be unknowingly interrupted. It is the only known method for transmitting a secret key over distance that is secure in principle and based on the law of physics.

Quantum Key Distribution (QKD) is the subset of quantum cryptography developed to transfer symmetric encryption keys between two locations. Quantum Key Distribution uses quantum mechanics to assurance secure communication. It enables two parties to produce a shared random secret key known only to them, which can then be used to encrypt and decrypt messages.

III. How Quantum Encryption Works

- Alice uses a light source to create a photon.
- The photon is sent through a polarizer and randomly given one of four possible polarization and bit designations-Vertical (one bit), Horizontal (zero bit), 45-degree right (one bit), or 45 degree left (zero bit).
- The photon travels to Bob's location.
- Bob has two beam splitters – a diagonal and vertical/horizontal – and two photon detectors.

International Research Journal of Innovations in Engineering and Technology (IRJIET)

ISSN (online): 2581-3048

Volume 3, Issue 11, pp 73-76, November - 2019

- Bob randomly chooses one of the two beam splitters and checks the photon detectors.

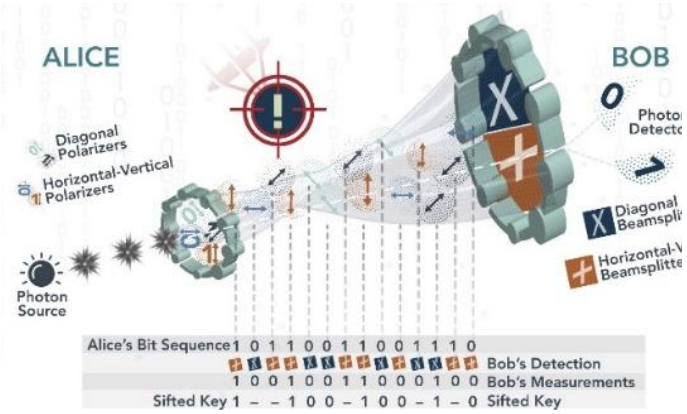

Figure 1: Quantum Encryption

- The process is repeated until the entire key has been transmitted to Bob.
- Bob then tells Alice is sequence which beam splitter he used.
- Alice compares this information with the sequence of polarizer she used to send the key.
- Alice tells Bob where in the sequence of sent photons he used the right beams splitter.
- Now both Alice and Bob have a sequence of bits (shifted key) they both know.

All in all, a pretty cool way of securely transferring an encryption key between two different locations.

IV. How Quantum Cryptography Works

In Quantum Cryptography, quantum channel construction requires a pair of polarizing filters at both sender and receiver ends. So, that at sender end we can send photons of selected polarization and at receiver end to measure the polarization of photons.

- The property of photons used in Quantum Cryptography is "Polarization".
- Polarization is the act of selecting light waves of a particular plane.
- Light moves in every plane.
- In linear polarization light can be polarized either horizontally or vertically.
- In circular polarization light waves are made to move in circular fashion.
- Linear and circular polarizations are bound with uncertainty.
- Measurement of linear polarization will destroy measurement of circular polarization.

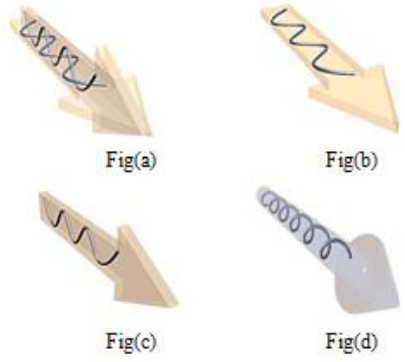

Figure 2: (a), (b), (c), (d) Quantum Cryptography

Quantum Key Distribution or Quantum Cryptography uses a series of photons (light particles) to transmit data from one location to another over a fiber optic cable. By comparing measurements of a fraction of these photons, the two endpoints can determine what the key is and if is safe to use.

Breaking the process down further helps to understand it better:

1. The sender transmits photons through a filter (or polarizer) which randomly gives them one of four possible polarizations and bit designations: Vertical (one bit), Horizontal (zero bit), 45-degree right (one bit), or 45 degree left (zero bit).
2. The photons travel to a receiver, which uses two beam splitters (horizontal/vertical and diagonal) to "read" the polarization of each photon. The receiver does not know which beam splitter to use for each photon and has to guess which one to use.
3. Once the stream of photons has been sent, the receiver tells the sender which beams splitter was used for each of the photons in the sequence they were sent, and the sender compares that information with the sequence of polarizers used to send the key. The photons that were read using the wrong beam splitter are discarded, and the resulting sequence of bits becomes the key.

If the photon is read or copied in any way by an eavesdropper, the photon's state will change. The change will be detected by the endpoints. In other words, this means you cannot read the photon and forward it on or make a copy of it without being detected.

V. Quantum Cryptography for Future Internet

Security for cyberspace in the future Internet should be guaranteed as it is the collection of all information systems and the information environment for human survival. For the

International Research Journal of Innovations in Engineering and Technology (IRJIET)

ISSN (online): 2581-3048

Volume 3, Issue 11, pp 73-76, November - 2019

growing security problem in cyberspace, quantum cryptography becomes the first consideration.

5.1 Unconditional Security

Cable and light are the main carriers of today's Internet communication. Alice and Bob are legitimate users in the system while Eve is an eavesdropper. In order to ensure security, they encrypt messages and then transmit it on the public channel.

In QKD model, sender wants to share a common conference key with his/her counterpart, which can be used to encrypt/decrypt messages they communicate. In QKD protocol, the real randomness of the key is guaranteed by the essential properties of the quantum: uncertainty principle. Moreover, an attacker is definitely detected if it exists.

5.2 Sniffing Detection

In quantum communication, the eavesdropper is sure to be detected because of quantum no-cloning theory. If an eavesdropper monitors quantum channel, for a bit of quantum information, he will choose the same measuring base with the sender with a 50% probability.

Therefore, the eavesdropper will be detected at a 50% probability for a bit of quantum information.

5.3 Security of the QKD

In order to simulate real situations in the future internet, we first analyze the quantum key distribution protocol in noise-free channel. Moreover, we further search the quantum key distribution protocol in noisy channel.

In order to analysis security of QKD protocol, we list the encoding of quantum information and the measurement bases. The two parties agree in advance that horizontal and the oblique downwards polarization represents "1" while the vertical and oblique upward polarization represents "0".

The probability of existence of a eavesdropper on the QKD protocol is as follows:

$Pr = Pr\{Base_A = Base_B \wedge Measure_A \neq Measure_B\}$

The probability that the eavesdropper is found for 1-bit quantum information is calculated ½*1/2*1/2=1/8

VI. Comparison between Cryptography and Quantum Cryptography

TABLE 1
Comparison between Cryptography and Quantum Cryptography

Classical Cryptography	Quantum Cryptography
It is based on Mathematical Computation.	It is based on Quantum Mechanics.
Bit rate depends upon computational power.	Average bit rate is 1MBPS.
Communication medium independent.	Communication medium dependent
Required up gradation as computing power increases.	It is based in physics law.

VII. Quantum Cryptography Applications

- Early this year, Chinese and Austrian researchers streamed the first quantum-encrypted video call.
- In 2017, Oxford University researchers, collaborating with Nokia and Bay photonics, created a system for transmitting quantum keys that could be used in POS systems.
- Switzerland has been using quantum cryptography to secure online voting since 2007.
- Battelle already uses quantum cryptography to protect the networks at its headquarters.

VIII. Conclusion

Compared with classical cryptography, its ultimate advantages are the unconditional security and the sniffing detection. These characteristics can solve cyberspace security critical problem for the future internet.

REFERENCES

Websites

[1] https://www.etsi.org

[2] https://www.academia.edu

[3] https://www.hindawi.com

[4] https://quantumxc.com

[5] https://www.techrepublic.com

ISSN (online): 2581-3048
Volume 3, Issue 11, pp 73-76, November - 2019

[6] http://www.apiit.edu.in
[7] https://www.sciencedirect.com
[8] https://www.geeksforgeeks.org
[9] https://www.researchgate.net
[10] https://ieeexplore.ieee.org
[11] https://www.plixer.com
[12] https://www.abebooks.com/.../charlie-kaufman-radia-perlman-mike-speciner
[13] https://en.wikipedia.org/wiki/Quantum_cryptography
[14] https://science.howstuffworks.com/.../quantum-cryptology.htm
[15] https://www.cryptography.wikia.com/wiki/Quantum cryptography
[16] https://www.williamstallings.com/Extras/Security-Notes/lectures/classical.html
[17] https://www.thefreelibrary.com/Quantum+Cryptography+for+the+Future+Internet+and+the...

Citation of this Article:

P. Sirsat, A. Nalamwar, "Quantum Communications and Cryptography" Published in *International Research Journal of Innovations in Engineering and Technology (IRJIET)*, Volume 3, Issue 11, pp 73-76, November 2019.

****

