Department of Computer Engineering

CSE 473 – Network and Information Security

Spring 2021 – 2022

Project Report

27.05.2022

Esra Eryılmaz

171044046

~ Quantum Cryptography ~

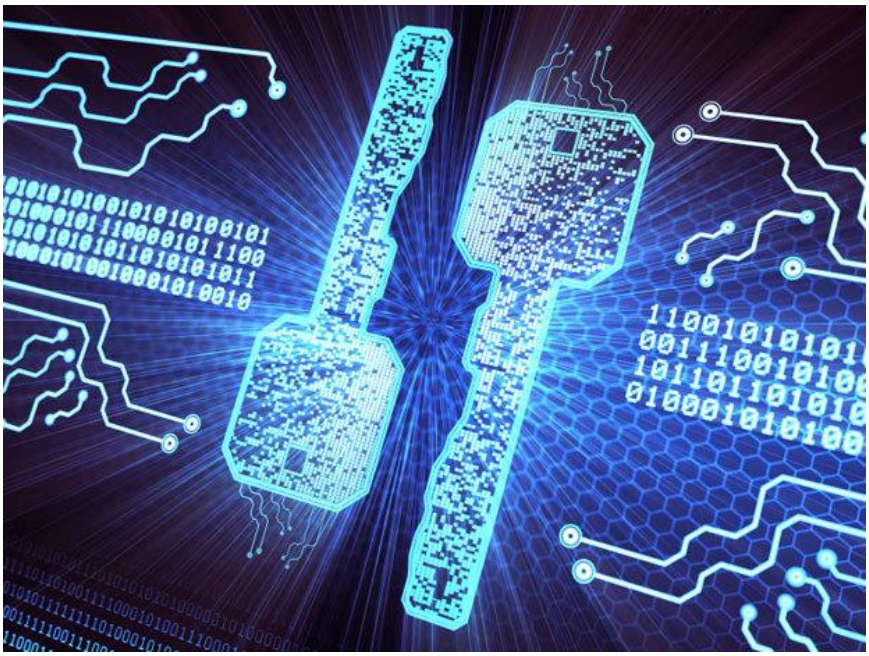
1) Introduction

This report includes my research on quantum cryptography. It is important to follow new technologies. Quantum cryptography is also an important topic at the moment. It is a topic that is not used much at the moment, but it is very useful and developing.

Quantum cryptography provides secure communication. Instead of difficult-to-crack numbers, quantum cryptography is based on the laws of physics, which is a more sophisticated and secure method of encryption.

It also provides detects eavesdropping. If a third party attempts to read the encoded data, then the quantum state changes, modifying the expected outcome for the users.

And it offers multiple methods for security. There are numerous quantum cryptography protocols used. Some, like QKD, for example, can combine with classical encryption methods to increase security.



2) Theoretical Explanation

- **Cryptography** is the art of devising codes and ciphers.
- **Crypto analysis** is the art of breaking them.
- **Cryptology** is the combination of the two i.e Cryptography and Crypto analysis.

Quantum cryptography is a science that applies quantum mechanics principles to data encryption and data transmission so that data cannot be accessed by hackers – even by those malicious actors that have quantum computing of their own.

- **History :**

Quantum cryptography attributes its beginning by the work of Stephen Wiesner and Gilles Brassard. In the early 1970s, Wiesner, then at Columbia University in New York, introduced the concept of quantum conjugate coding. His seminal paper titled "Conjugate Coding" was rejected by the IEEE, but was eventually published in 1983 in SIGACT News. [1]

In that paper he showed how to store or transmit two messages by encoding them in two "conjugate observables", such as linear and circular polarization of photons, so that either, but not both, of which may be received and decoded.

Quantum cryptography is the art and science of exploiting quantum mechanical effects in order to perform cryptographic tasks. While the most well-known example of this discipline is quantum key distribution (QKD), there exist many other applications such as quantum money, randomness generation, secure two- and multi-party computation and delegated quantum computation. [3]

Also the goal of post-quantum cryptography (also called quantum-resistant cryptography) is to develop cryptographic systems that are secure against both quantum and classical computers, and can interoperate with existing communications protocols and networks. [4]

Differences between traditional cryptography and quantum cryptography :

Unlike traditional cryptography, which is based on mathematics, quantum cryptography is based on the laws of quantum mechanics.[15]

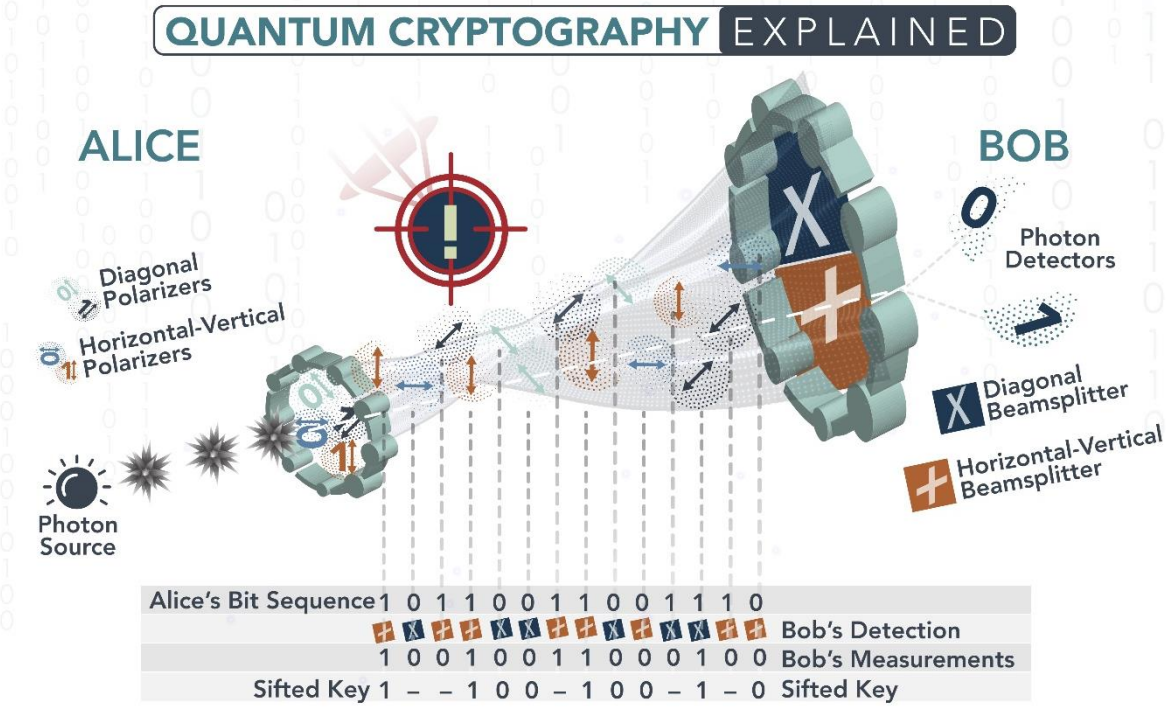
Classical cryptography	Quantum cryptography
Uses logic based on digital logic	Is based on quantum theory
Sends digital signals using bits	Sends data through the use of particles or photons
Typically doesn't have a range associated with it	Typically has a range associated with it that requires fiber optic wires and repeaters
Encryption is based on mathematical algorithms	Encryption is based on quantum properties

How does quantum cryptography work?

In theory, quantum cryptography works by following a model that was developed in 1984.

The model assumes there are two people named Alice and Bob who wish to exchange a message securely. Alice initiates the message by sending Bob a key. The key is a stream of photons that travel in one direction. Each photon represents a single bit of data -- either a 0 or 1. However, in addition to their linear travel, these photons are oscillating, or vibrating, in a certain manner. [6]

So, before Alice, the sender, initiates the message, the photons travel through a polarizer. The polarizer is a filter that enables certain photons to pass through it with the same vibrations and lets others pass through in a changed state of vibration. The polarized states could be vertical (1 bit), horizontal (0 bit), 45 degrees right (1 bit) or 45 degrees left (0 bit). The transmission has one of two polarizations representing a single bit, either 0 or 1, in either scheme she uses.



The photons now travel across optical fiber from the polarizer toward the receiver, Bob. This process uses a beam splitter that reads the polarization of each photon. When receiving the photon key, Bob does not know the correct polarization of the photons, so one polarization is chosen at random. Alice now compares what Bob used to polarize the key and then lets Bob know which polarizer she used to send each photon. Bob then confirms if he used the correct polarizer. The photons read with the wrong splitter are then discarded, and the remaining sequence is considered the key.

Let's suppose there is an eavesdropper present, named Eve (attacker). Eve attempts to listen in and has the same tools as Bob. But Bob has the advantage of speaking to Alice to confirm which polarizer type was used for each photon; Eve doesn't. Eve ends up rendering the final key incorrectly.

Alice and Bob would also know if Eve was eavesdropping on them. Eve observing the flow of photons would then change the photon positions that Alice and Bob expect to see.

3) Details of Some Articles

Here, I have discussed 4 of the basic quantum cryptography studies which are cyber security, medical, online banking system and big data,

- **Applications of quantum cryptography in Cyber Security:**

  The advantages present in the quantum computers will make the public keys like RSA, Ellamae and other public keys will no longer be safer in the quantum computers. Also, problems like Discrete logarithm problem or integer factorization can be easily solved using quantum computers. So in order to secure these systems we need different cryptosystems which are not based on the above problems.

  Both network security and Cryptography are key in ensuring the safe security of the information systems. One of the main essentials of Cyber security is to explore the quantum cryptographic protocols. [7]

- **Applications of quantum cryptography in Medical :**

  A novel enhanced BB84 quantum cryptography protocol provides strong security on the wireless body sensor networks in healthcare applications. Significant works have been done to ensure secure communication in the WBSN.

  In the future, our scheme should include a more mathematical and computational process of quantum key generation for protecting healthcare information in the wireless communication medium. [8]

- **Applications of quantum cryptography in Online Banking System:**

  Security for online banking has changed considerably during the relatively short period that online banking has been in use. In particular, authentication in the early implementations was, and sometimes still is, vulnerable to various attacks such as phishing. It is

known that the quantum cryptography protocols are able to detect immediately any attempt to attack the key exchange and the authentication process.

In the paper they propose a model for authentication in online banking system with quantum cryptography.[9]

- **Applications of quantum cryptography in Big Data :**

Enhancement of security and privacy in mobile data centers is challengeable with efficient security key management. In order to solve this problem, data centers need efficient quantum cryptography using Grover's algorithm and authentication technique which are appropriate approaches to enhance the security and privacy with less complexity.

Quantum cryptography with the PairHand protocol seems to be a better approach. In future, light which has same quantum properties will be the best approach because people can see only the light not the data. So, light based on quantum cryptography and PairHand protocols will be the best for that research. [10]

4) Conclusion and Recommendations

Conclusion :

- Quantum cryptography promises to revolutionize secure communication by providing security based on the fundamental laws of physics, instead of the current state of mathematical algorithms or computing technology.

- The devices for implementing such methods exist and the performance of demonstration systems is being continuously improved.

- Within the next few years, if not months, such systems could start encrypting some of the most valuable secrets of government and industry.

Recommendations :

Solutions to this problems can be search :

For now, computers capable to transmitting information using quantum cryptography are very large, custom-made and, thus, expensive. A couple of banks have already taken advantage of this security method, but few other organizations would be able to afford it in the foreseeable future.

With regards to entangled photons, which seem to be absolutely safe, there is also a serious practical problem not only with the cost, but also with keeping them entangled long enough to meet the needs of the real world. While the system is perfect in theory, it is going to be very hard to implement it in practice.

Another problem is that for distances beyond 50 kilometers or so, the noise becomes so great that error rates skyrocket. This not only leaves the channel very vulnerable for eavesdroppers, but also makes it virtually impossible to send information. However, it is potentially possible for quantum keys to be exchanged through the air in the future. Tiny telescopes would then have to be aligned to detect the signal. Some calculations even suggest that photons could be detected by a satellite, which would allow communication between continents!

For the future all we need is some years, or maybe decades or even centuries, to refine the technique and make it practical in the real world.

Also it can be worked on to reduce the high cost of quantum cryptography system.

Bibliography

[1] Bennett, Charles H., et al. "Quantum cryptography, or unforgeable subway tokens." *Advances in Cryptology*. Springer, Boston, MA, 1983.

[2] Pirandola, Stefano, et al. "Advances in quantum cryptography." *Advances in optics and photonics* 12.4 (2020): 1012-1236.

[3] Broadbent, Anne, and Christian Schaffner. "Quantum cryptography beyond quantum key distribution." *Designs, Codes and Cryptography* 78.1 (2016): 351-382.

[4] Chen, Lily, et al. *Report on post-quantum cryptography*. Vol. 12. Gaithersburg, MD, USA: US Department of Commerce, National Institute of Standards and Technology, 2016.

[5] Bernstein, Daniel J., and Tanja Lange. "Post-quantum cryptography." *Nature* 549.7671 (2017): 188-194.

[6] Tomamichel, Marco, et al. "Tight finite-key analysis for quantum cryptography." *Nature communications* 3.1 (2012): 1-6.

[7] Sharbaf, Mehrdad S. "Quantum cryptography: An emerging technology in network security." *2011 IEEE International Conference on Technologies for Homeland Security (HST)*. IEEE, 2011.

[8] Anusuya Devi, V., and V. Kalaivani. "Enhanced BB84 quantum cryptography protocol for secure communication in wireless body sensor networks for medical applications." *Personal and Ubiquitous Computing* (2021): 1.

[9] Sharma, Anand, and S. K. Lenka. "Authentication in online banking systems through quantum cryptography." *Int. J. Engineering and Technology* 5 (2013): 2696-2700.

[10] Thayananthan, Vijey, and Aiiad Albeshri. "Big data security issues based on quantum cryptography and privacy with authentication for mobile data center." *Procedia Computer Science* 50 (2015): 149-156.

[11] Elliott, Chip. "Quantum cryptography." *IEEE security & privacy* 2.4 (2004): 57-61.

[12] Gisin, Nicolas, et al. "Quantum cryptography." *Reviews of modern physics* 74.1 (2002): 145.

[13] Bennett, Charles H., Gilles Brassard, and Artur K. Ekert. "Quantum cryptography." 267.4 (1992): 50-57.

[14] Yati, Maneesh. (2020). Quantum Cryptography. 10.13140/RG.2.2.34447.61601.

[15] https://www.techtarget.com/searchsecurity/definition/quantum-cryptography

[16] https://en.wikipedia.org/wiki/Quantum_cryptography