A BRIEF EXEGESIS ON QUANTUM CRYPTOGRAPHY

✍ **Niraj Raj Adhikari**

HR Manager, CSAN

1.ABSTRACT

How do you ensure your data is secure? How do you know no one can see what you buy online, send a private Twitter message, or conduct an online banking transaction? You don't, at least not for certain. You, on the other hand, have faith in the encryptions that keep it safe. However, how reliable are these encryptions? The keys that protect your banking information are obviously more difficult to crack, but they may not be for much longer. The enormous amount of time and processing power required to break these codes makes them practically impregnable. It would take nearly 12 million times the age of the universe if all of the world's personal computers worked nonstop to break the coding that protects email. Contemporary computers, on the other hand, can be soon supplanted by quantum computing, which can accomplish tasks that would take billions of years for modern computers in days or hours. There would be no such thing as a safe secret. However, researchers are prepared for this. They have already created a new sort of encryption that's not only tough but also impossible to crack. It's referred to as **Quantum Cryptography*.**

The core purpose of this article was to interpret **Quantum Cryptography** and to get the information on its relevance. The exegesis of this article briefly explains its concept, working principle, applications, advantages, limitations.

***Cryptography**- The art or science encompassing the principles and methods of transforming an intelligible message into one that is unintelligible, and then transforming that message back to its original form.

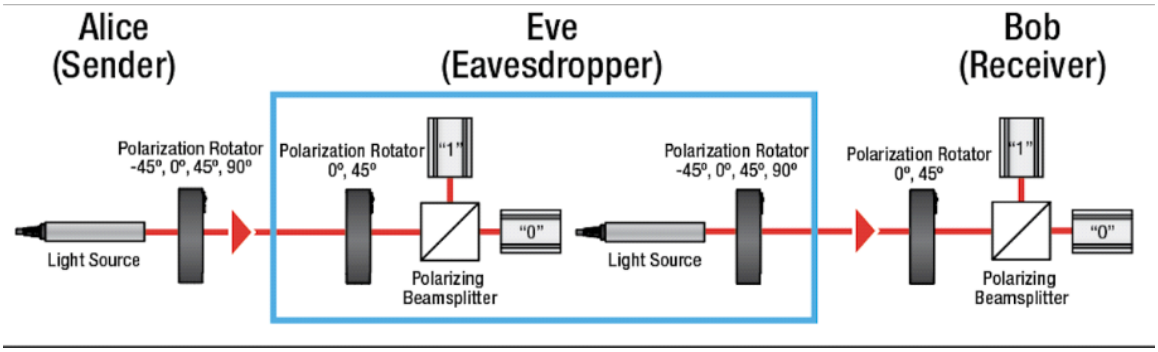
2.ORIGIN OF CONCEPT OF QUANTUM CRYPTOGRAPHY

The study of quantum physics was advanced via the efforts of many physicists after the German physicist Max Planck initially introduced the idea of a quantum in 1900. By the 1930s, a pretty complete set of theories of quantum mechanics had been produced. Quantum cryptography is based on the principles of quantum mechanics, in contrast to traditional public key cryptography, which is based on the

computational complexity of specific mathematical functions and cannot prove that eavesdropping has occurred at any point during the communication process or that reversing the one-way functions used is actually difficult mathematically. Stephen Wiesner, a personnel at Columbia University in New York, initially put up the idea of quantum cryptography after he introduced the ideas of quantum money and quantum conjugate coding in 1968. A secure communication technique based on Wiesner's conjugate observables was proposed by Gilles Brassard of the University of Montreal and Watson Research Center. A novel method for quantum key distribution was invented in 1991 by Artur Ekert, who was a PhD candidate at Wolfson College, University of Oxford. This method is based on the distinctive quantum correlations known as quantum entanglement. Quantum cryptography attracted increased interest in the 1990s as the advent of quantum algorithms and quantum computing threatened the status quo public key cryptography.

3.HOW QUANTUM CRYPTOGRAPHY WORKS?

Quantum cryptography uses the laws of quantum physics to transmit private information in a way that makes undetected eavesdropping impossible. A series of photons are used to convey a secret, random sequence known as the key in quantum key distribution (QKD), the most extensively researched and practical form of quantum encryption. By comparing measures collected at either end of the transmission, users will know if the key has been compromised. Without the callers' knowledge, someone who wiretapped a phone may intercept a secret code. In contrast, there is no way to "listen in" on or monitor a quantum encrypted key without disrupting the photons and affecting the outcomes of the measurements at each end. This is due to a law in quantum mechanics called the **uncertainty principle***, which says that the act of measuring a property of a quantum system may alter some of the other properties of the quantum object (in this case, a photon).



Fig(i): Working of Encryption using quantum Physics

***Uncertainty Principle**- In quantum mechanics, the uncertainty principle (also known as Heisenberg's uncertainty principle) is any of a variety of mathematical inequalities asserting a fundamental limit to the accuracy with which the values for certain pairs of physical quantities of a particle, such as position 'x',

and momentum 'p', can't be predicted from initial conditions.

In other words, if you measure one thing, you cannot measure another thing accurately. For example, if you apply this principle to humans, you could measure a person's height, but you can't measure his weight. The only odd thing about this principle is that it becomes true only for the instant at which you try to measure something. This principle applies to the photons. Photons have wave-like structure and are polarized or tilted in a certain direction. While measuring photon polarization, all subsequent measurements are getting affected by the choice of measures that we made for polarization. This principle plays a vital role in preventing the efforts of attackers in quantum cryptography.

4.APPLICATIONS & PROTOCOLS

I. Quantum Key Distribution

The best-known example of how our modern society uses quantum cryptography is quantum key distribution (QKD). This protected communication method enables the secure distribution of secret keys known only by the authorized parties. QKD allows the two communicating users to detect the presence of any third party trying to "look" at the key. Using quantum superpositions or quantum entanglement and transmitting information in quantum states, a communication system can be implemented that detects any attempts at spying.

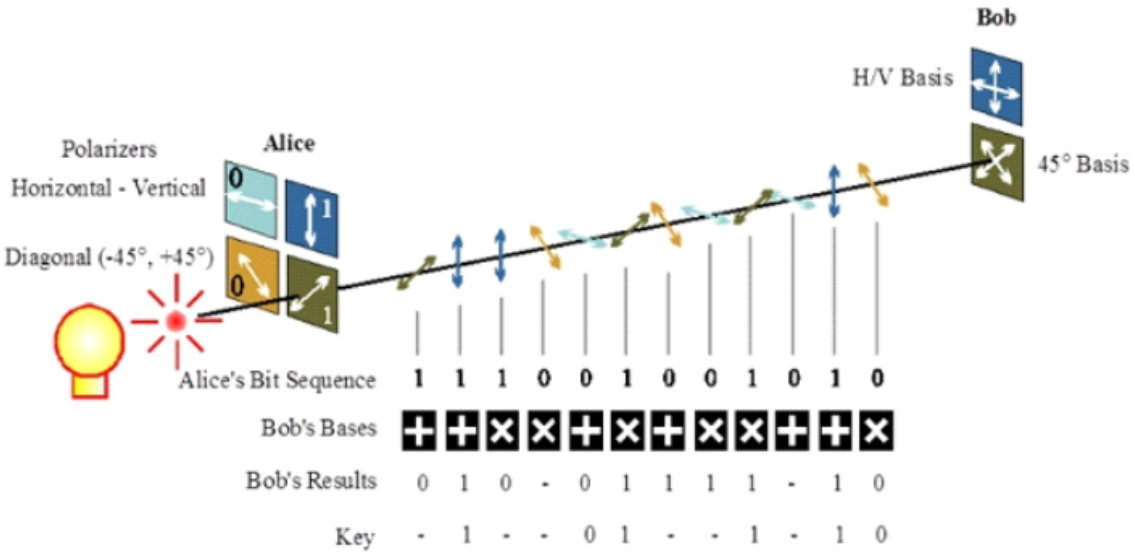


Fig (ii): QKD system using BB84 protocol

Quantum key distribution allows only the production and distribution of a key, not transmitting any message data. This key can then be used in conjunction with an encryption algorithm to encrypt (and decrypt) a message.

II. Mistrustful Quantum Cryptography

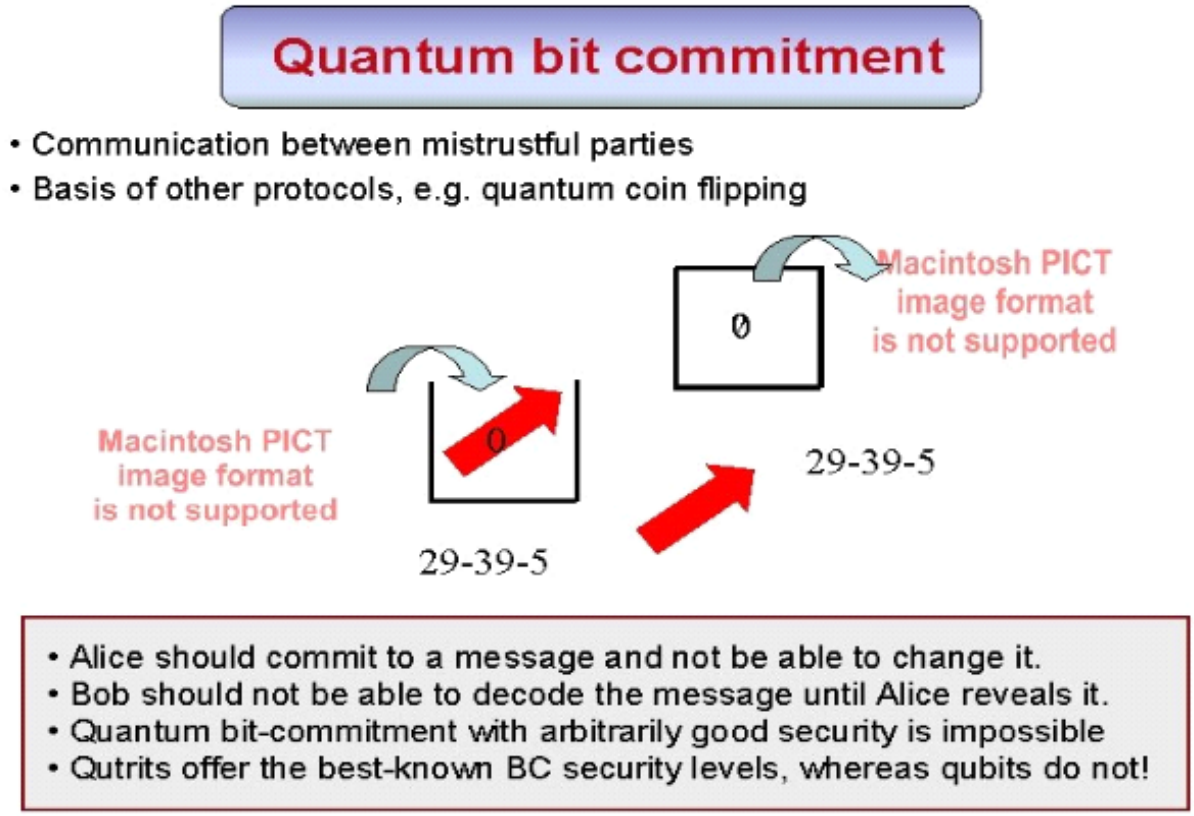
What should you do when you're unsure of the trustworthiness of another participating party? This is where mistrustful quantum cryptography comes in. When both parties need reassurance that the opposite side is engaging with good intention, then mistrustful quantum cryptography is an excellent solution.

Let's look at an example.

Bob and Alice are collaborating, and the project requires personal input from both parties, but neither party has a guarantee that the other won't cheat. Examples of tasks in mistrustful cryptography are commitment schemes (which allows one to commit to a chosen value while keeping it hidden to others) and secure computations (which enables parties to jointly compute a function over their inputs while keeping those inputs private).

III.Quantum Commitment

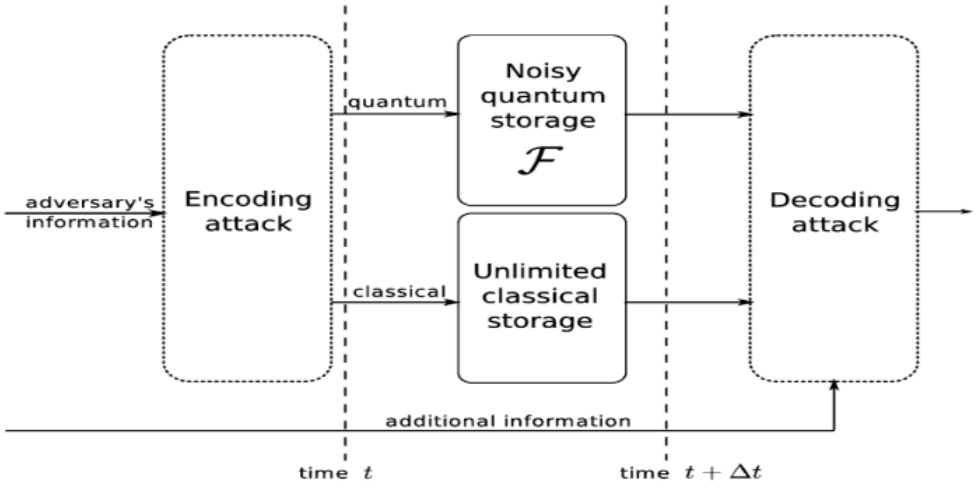
A commitment scheme (mentioned under mistrustful quantum cryptography) allows a party to commit to a specific value. The sender cannot change the fixed value, and the recipient cannot learn anything about the value until the sender reveals it. Such commitment schemes are commonly used in cryptographic protocols like quantum coin flipping, zero-knowledge proof, secure two-party computation, and oblivious transfer.



Fig(iii): Quantum bit commitment

IV.Bounded- And Noisy-Quantum-Storage Model

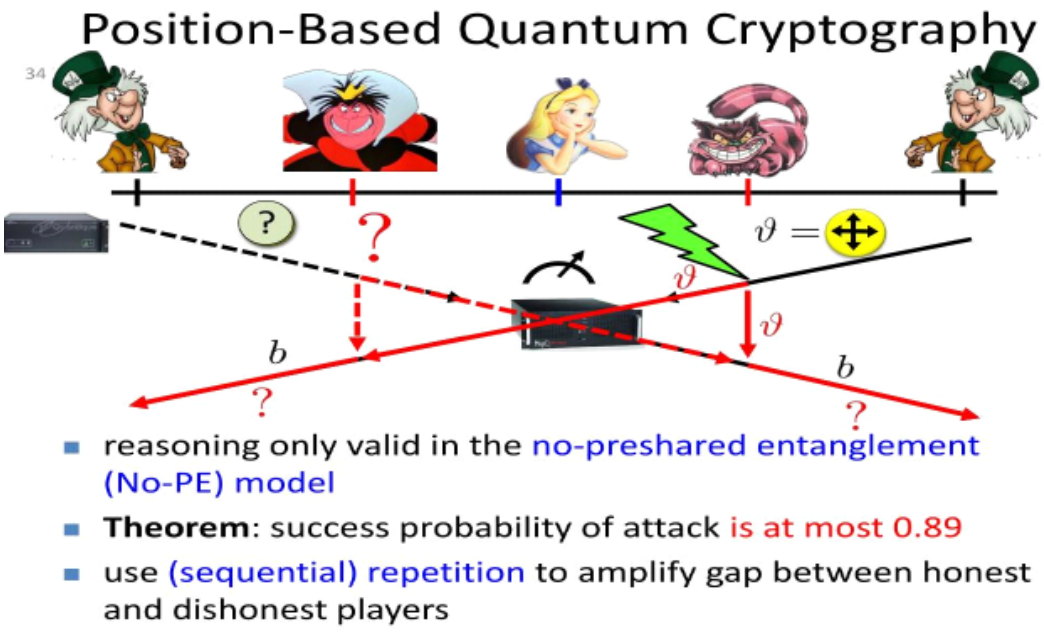
In the bounded quantum storage model, or BQSM for short, there is an assumption that some known constant Q limits the amount of quantum data that an adversary can store. The protocol parties exchange more than Q qubits, and since storage is limited, a large part of the transferred data must either be measured or discarded. Forcing dishonest parties to measure a large part of the data allows the protocol to circumvent the impossibility result.



Fig(iV): Noisy quantum Storage model

V. Position-Based Quantum Cryptography

Here the geographical location of a player is used as its (only) credential. For instance, a participant sends a message to the receiving party at a known position to guarantee that the recipient can only read the data at the specified location. Under the name of “quantum tagging”, the first position-based quantum schemes were investigated in 2002.. After that, the U.S. granted a patent in 2006, and the notion of using quantum effects for location verification first appeared in the scientific literature in 2010.



Fig(v): Position-Based Quantum Cryptography

VI. Measurement-Device-Independent Quantum Cryptography

A unique protocol, often referred to as MDI, removes all attacks from the detection system, the most vulnerable part in many cryptographic implementations. As a result, security is held independently of the quality of the underlying physical devices. This unique property makes measurement-device-independent quantum cryptography a good candidate for protection against malicious devices.

VII.The BB84 Protocol

In 1984, Charles Bennett and Gilles Brassard published a protocol based on Heisenberg's uncertainty principle. The protocol is named BB84 after the authors' names and the year it was published. It is one of the most prominent quantum protocols. All the other protocols based on HUP are considered variants of BB84. In the BB84 protocol, Alice can transmit a random secret key to Bob by sending a string of photons with the private key encoded in their polarization. The no-cloning theorem guarantees that Eve cannot measure these photons and transmit them to Bob without disturbing the photon's state in a detectable way. The above is true, considering no error on the quantum channel. If the track is prone to error, Alice and Bob will not detect Eve's presence all the time.

5.ADVANTAGES & BENEFITS:

Quantum Cryptography is advantageous over Classical Cryptography in aspects as pointed below.

- **Virtually unhackable**- Unlike mathematical encryption, quantum cryptography uses the principles of quantum mechanics to encrypt data and make it virtually unhackable.
- **Gives the Solution needed now for tomorrow-** As the need for unbreakable encryption looms in networks around the world, quantum cryptography is the solution that will safeguard and future-proof sensitive information.
- **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.
- **Detects eavesdropping-** If a third party attempts to read the encoded data, then the quantum state changes, modifying the expected outcome for the users.

6.DISADVANTAGES & LIMITATIONS

There are some problems while using quantum states to transmit information. Some of them are listed below.

- **Point to Point links and Denial of Service**- The quantum channel is a point to point connection that is 1:1 connection. To link N number of nodes, N(N-1)/2 links will be required which increase cost and maintenance overhead. If an attacker cuts the physical link, Dos attack takes place.
- **High Bit Errors Rate**- The bit error rate of a quantum key distribution is higher than an optical communication system. The Error control protocol called CASCADE is used to correct bit errors, but it further makes the system vulnerable to new attacks. The CASCADE leads to the problem of leakage of bits of secret key which is nullified by the process Privacy Amplification. Privacy amplification performs a compression function on the bit error corrected key. This will guarantee that the bits leaked to the attacker will become useless and both communicating parties will have the same key.
- **Losses in the Quantum Channel**- Free space quantum channels suffer from the atmospheric and equipment dependent geometric losses. Quantum signals cannot be amplified therefore; the losses on the channel will be too high to distinguish the readings from dark count rates.
- **Classical Authentication**- Quantum cryptography does not provide the digital signature as in classical cryptography and related features, such as certified mail.

7.CONCLUSION

It is remarkably simple to integrate quantum cryptography, a new technology that depends on quantum physics phenomena. Many businesses have created quantum cryptography prototypes because of their very secure key distribution, really random key generation, faster key refresh rate, and proactive infiltration. The experimental quantum cryptography systems have experienced enormous advancements in recent years. Therefore, quantum cryptography offers significantly higher levels of security in key distribution than traditional encryption, which relies on mathematical principles. There are many quantum cryptography algorithms available. Despite having many benefits, it has significant drawbacks as well, such as a high bit error rate and losses in the quantum channel. This means, in theory, quantum cryptography seems to be a successful turning point in the information security sector. However, no cryptographic method can ever be absolutely secure. In practice, quantum cryptography is only conditionally secure, dependent on a key set of assumptions.

8.REFERENCES

- https://www.youtube.com/watch?v=uiiaAJ3c6dM
- https://www.mpiwg-berlin.mpg.de/research/projects/origin-and-development-quantum-cryptography#:~:text=Quantum%20cryptography%20was%20first%20proposed,money%20and%20quantum%20conjugate%20coding.
- https://scienceexchange.caltech.edu/topics/quantum-science-explained/quantum-cryptography
- https://en.wikipedia.org/wiki/Uncertainty_principle
- https://www.geeksforgeeks.org/classical-cryptography-and-quantum-cryptography/
- https://quantumxc.com/blog/quantum-cryptography-explained/
- http://www.ijarse.com/images/fullpdf/1524848399_JK1640IJARSE.pdf