Quantum Cryptography: A brief review of the recent developments and future perspectives

Azeem Iqbal Muhammad Junaid Aslam Hafiza Sahar Nayab
University of Management and Technology
C-II Johar Town Lahore
azeem.iqbal@lums.edu.pk

ABSTRACT

Quantum Cryptography is a novel approach to make the information and network world more secure. Unlike classical cryptography, quantum cryptography ensures the security of communication because it is based on the laws of Quantum Mechanics: a branch of physics that deals with the fundamental behavior of matter and their energies to the levels of subatomic particles. These particles and their intrinsic properties such as photon polarization and entanglement allow us to develop an unbreakable system of cryptographic information. Conventionally, the security has been primarily concerned with the secured distribution of secret key carried over an insecure channel. However, in Quantum Cryptographic systems the transmission of secret key is done using aforementioned laws of nature through a secured quantum channel highly susceptible to intrusion detection. Consequently, the Quantum Key Distribution (QKD), in conjunction with protocols such as BB84 protocol has emerged as an ultimate modern secured communication system. This article concentrates on briefly reviewing quantum cryptography, some recent developments and reports of its vulnerabilities.

KEYWORDS

Quantum cryptography – Principles of Quantum Cryptography – Recent Developments in Quantum Cryptography – Future of Quantum Cryptography

INTRODUCTION

The advent of modern communication has lead to the globalization of our societies. People are more connected today than ever in the history of mankind. This ability of consistent interaction without constraints of distances has produced many benefits but at the same time has raised concerns for the privacy and security of the sensitive information they communicate to each other. This was the prime source of concern at the time when network communication was solely being used for military purposes and the sensitive information was prone to getting intercepted by enemy hackers. To overcome this problem cryptography was developed. It is a method to transform plaintext into an encrypted modified text called cipher text that is send over the traditional unsecured communication channel and at the received end is reversed to achieve back the plaintext, thus completing the communication process.

Primarily, two forms of modern cryptographic techniques are used, Public key encryption (PKE) and Secret key encryption (SKE). The risk in either ones is that loosing the encryption key breaks the system and thus finding an effective mechanism for the key distribution led to the development of quantum cryptography.

1 HISTORY

Quantum cryptography was first proposed by Stephen Weisner in his work “Conjugate Coding” in the early 1970s [1]. The article highlighted the laws of quantum mechanics that could create bank notes that were impossible to counterfeit. This primal approach of Wiesner perpetuated into the innovative concept of the new form of public-key cryptography termed as the “Quantum Cryptography” [2]. Although, it was considered to be highly unrealistic due to the intrinsic nature of photons, Wiesner was already using it in his multiplexing scheme. However, his work was not accepted for publication and was revived in 1979, by Bennett and Brassard. Their motive towards such scheme was that it could fundamentally be used in the transmission of quantum states of photons via a quantum channel. Initially, the idea came up with a quantum encryption scheme that was much related to the conventional one-time-pad but it was still not very practical. In 1983, Bennett and Brassard had to leave their scheme because they came up with an idea of transmitting encryption key over the quantum channel rather than the actual message. It turned out
to be a much simpler approach to securely transmitting a random key, once transmitted, algorithms such as the one-time-pad could be used to decrypt the actual message in the standard method. Eventually, in 1983 this heuristic work was accepted in an information-theory conference and led to the foundation of Quantum Key Distribution (QKD) [3] and Brassard took this work to publication with the full description of their QKD scheme which later on formulated itself as the BB84 QKD scheme [4].

2 PRINCIPLES OF QUANTUM CRYPTOGRAPHY

2.1 Entanglement
A phenomenon that generates quantum state of fundamental particles in such a way that they cannot be defined independently. Firing a laser through a crystal and splitting a single photon into two can allow one to create entangled photons. Intuitively, by the laws of physics, their state is intact and disturbing one will instantly disturb the other regardless of the distance. In case of quantum cryptography, this has been very useful in secured communication as it easily allows us to detect the presence of an eavesdropper. Technically, a photon generator placed between Alice and Bob at the same time sends pairs of entangled photons with the same polarization to Alice and Bob. Both measure the signals with an alternating random bases and after the comparison discard the bits the are measured with different bases. The phenomena of entanglement allows this communication to remain ultimately secured as any activity to intrude on either one of the states will immediately affect the other allowing detection of an eavesdropping.

2.2 Photon Polarization
Light is classically defined as an oscillating electromagnetic wave with magnetic and electric fields. Today, we know that it contains discrete packets of energy termed as "Photons". Polarization is holistically, the means orientation as it originates from the Greek word “polos”, the axis of a spinning globe. The quantum superposition of eigenstates create different types of polarizations such as linear, circular or elliptical. Further, these photons carry energy, momentum as well as an angular momentum. The classical Maxwell’s equations is used to determine the probability for a photon to be in a particular polarization state. This serves as the fundamental step in creating the security state of information transport as depicted in an experiment by (Poppe et al.).

2.3 Heisenberg Uncertainty Principle
The uncertainty principle is a simple probabilistic relationship of the measure of position $x$ and the momentum $p$ of a particle with no absolute precision. It says that the more accurately we know any one of this value the very less we know the other. In the combination of their uncertainty, it generates a number the is greater than or equal to half of Planck’s constant $\hbar$. Mathematically, the uncertainty principle is depicted as,

$$\Delta x \Delta p \geq \frac{\hbar}{2} \quad (1)$$

3 QUANTUM CRYPTOGRAPHY PROTOCOLS

3.1 BB84
Although several exist, a single quantum cryptography protocol is sufficient to illustrate the principle of quantum cryptography, the BB84 protocol. As described earlier it was the first Quantum Cryptographic protocol invented in 1984 by Charles Bennett of IBM Research and Gilles Brassard of the University of Montreal. [4].

It is still a widely used protocol and primarily serves as a basis for understanding the quantum cryptographic practical applications. It begins with an emitter and a receiver (connected via an optical fiber) using four different polarization states to encode bit values, a 0 deg-bit as horizontal, a 45 deg diagonal or as a +45 deg-bit value with either a vertical or a -45 deg diagonal state. The emitter sends photons with random polarization selected among the four of them. The random orientations are recorded in a list and the photons are sent along the quantum channel. For the incoming photons, random orientation of the states filter allow us to distinguish in between the two polarization states of photons. These orientations are an outcome of the detected photons.

4 RECENT DEVELOPMENTS

4.1 Hyperentanglement
In previous studies, photons were typically entangled in one dimension of their own quantum properties which is usually the direction of their polarization. In a recent study [15], it has been demon-
strated that the photons can be sliced and entangled as a pair with multiple dimensions of quantum properties such as the spin and energy. The method has been referred to as hyperentanglement [6] and it has enabled each photon pair to carry much more data than previously possible. The users now have the enormous ability to send much denser packets of information using the same networks. Progressively, it has been used in developing a quantum key distribution (QKD) system with high photon efficiency and increased rate of data transfer. The photons entangle in polarization, spatial mode, and time-bin degrees of freedom (DOF) using spontaneous parametric downconversion (SPDC) in a pair of nonlinear optical BiBO crystals.

4.2 Quantum cryptography with twisted light

The quantum systems for key distribution heavily rely on the polarization state of light for encoding and decoding information. This limits the amount of information that could be sent per photon. In a recent study, researchers have finally developed a way to transfer 2.05 bits per photon by using twisted light. [16]. It has been made possible by taking into account both the orbital angular momentum of the photons and their angular position for encoding the information. The encoding and decoding of information has been tested to be around at the rate of 4kHz with 93% accuracy. This work has revealed a new paradigm towards realizing the multi-level quantum communication systems which would be able to record and store data at much higher capacities and levels of great security.

4.3 Long-Distance Teleportation

A team of researcher using ESAs Optical Ground Station located in the vicinities of Canary Islands have recently set a new distance record in quantum teleportation by reproducing the characteristics of a light particle across 143 km of open air. [17] It is made possible by creating two entangled photons using Bell-state measurement. This system intuitively gives more evident security advantage over the photon polarization methodology. Instead of using a weak laser pulse to polarize and send photon packets, it is possible to simply build an entangled quantum key distribution system. As researchers draw close to achieving higher distances, quantum reexportation is a potential applicant of quantum cryptography.

4.4 Vulnerabilities

4.4.1 Loophole in free space

In free-space the sensitivity of the receiver’s detector channels depend on the spatial mode of incoming photons. This makes it very easy for the attacker to control the spatial modes and break the proclaimed security in a quantum cryptographic system [18]. The experimental investigation has revealed that a receiver of the QKD, in a standard mode of polarization system, should be able to identify the source efficiency that is a mismatch with its optical scheme. In a recent test, the intercept-and-resend attack has shown that the system is breakable in most situations.

4.4.2 Violation of Bell test

Photonic systems based on energy-time entanglement are subjected to prove their security at a local regime using the Bell inequality test. It certifies the security of device-independent quantum key distribution (QKD). The work done by (Jogenfors et al.), in this regard, exhibits how this can be tested using standard avalanche photodetectors. The work shows that it allows an attacker to breach a quantum cryptographic system without even leaving a single trace. This first ever demonstration of a violation-faking source gives the system both a violation setting that can be altered as required and a high end faked detector efficiency. Briefly, the Device-independent Bell inequality violation should be performed with care to avoid loopholes. This also has the distinct advantage over polarization and so can more easily communicate over long

Figure 1. The Quantum Key Distribution System using BB84 Protocol
distances than polarization. Consequently, energy-time entanglement is being preferred as the next quantum artifice to perform the reliable key distribution.

5 FUTURE PERSPECTIVES

The future development in quantum cryptography is certainly towards increasing the key exchange rate and efficiency of the information transmitted. A proposal is to get rid of the optical fiber, replacing it with a terrestrial station that would allow the use of a low orbit satellite station for the transmission. Some research groups have already performed preliminary tests of such systems, but an actual key exchange with a satellite system remains to be demonstrated. Several theoretical proposals for building quantum repeaters are being proposed which would heavily rely on the quantum bits. The development of commercial quantum computers is predicted to create a huge outburst for the practical implementations of quantum cryptography over transcontinental distances.

6 CONCLUSION

There is no debate about the fact that quantum cryptography is a truly breakthrough field and under research. Though there are imperfections and the technology still has its own constraints towards commercial implementations, it has seen a tremendous growth recently. Consequently, we should realize that fundamental knowledge of such systems is an important element of the future. Computer scientists must understand these fundamental laws of nature to be able to develop new algorithms and new distribution schemes for its practicality. All we need now are a few more years to finally bring the realms of this technology to the commercial and consumer world.

REFERENCES


