Quantum Cryptography

(author list is on the last page)

Introduction

Efforts have been put into keeping information security for different purposes. Throughout history, cryptography, the craft of hiding messages, has evolved from simple tricks to a whole delicate subject. In this digitizing era, we are still relying on mathematical coding. Encryption involves tremendous complication but the core principle remains the very same. But with insights brought by physics, encryptors can now resort to quantum effects to bring about the highest security ever to information. *Quantum cryptography* comes to play.
Unlike traditional cryptography, in which you get nothing or otherwise everything, quantum cryptography allows you to steal a tiny amount of content if you are lucky enough. However, such an attempt to hijack a connection will be detected immediately. So, that's nearly impossible for the key to get stolen. To begin our journey, let's see how the cryptography has evolved.

A brief history of cryptography

Cryptography has been the using of *mathematical algorithms* to transform some data into an unreadable form by symbols substitution, this new form can only be decrypted with a correct key that is known to both the sender and receiver.
We could make a distinction between *classical cryptography* and *modern cryptography*.

Classical Cryptography
Classical Cryptography can be understood as a simplistic try on securing message by *symbol substitution* or *transformation*. For example, the alphabets I, U, A are frequently rotated in the encrypted message, which makes the message becoming unreadable to others hence be more secure.
Messages encrypted in this way could be decrypted by "trials and errors". If the key is unknown and the way of substitution is obscure, it is quite an unbreakable way of securing information. During the Second World War, information security was a must for both the Allies and Axis, and this pushed the evolution of cryptography.
Without much advance in algorithm, encryptions were complicated by machines *mechanically* and *electro-mechanically* at that period. The machines were fast and reliable so that secure and detailed messages can be delivered.

Modern Cryptography
Modern Cryptography rose by the end of the Second World War, the paper "Communication Theory of Secrecy System" by Claude Shannon, described several advanced and complex algorithms for cryptography. Since then, these algorithms for securing messages, themselves, were secured by intelligence agencies such as National Security Agency.
Cryptography resurfaced to the public, when IBM published the Data Encryption Standards (DES) to reinforce business security, like bank industry, in 1975. DES included several complicated encryption process and standardized encryption. Some variants like AES, TDES were also set up later.

Though for both classical and modern cryptography, there is a risk of being eavesdropped. A spy between the receiver and the sender can easily deceive the receiver with a "faked" public key of the sender. Since the spy knows the real public key of the sender, once the receiver send back a

secret message to the sender using the “faked” public key, the spy can decrypt using his/her own private key and re-encrypt it with the sender’s public key. Such a spying would not be discovered easily. Messages are at risk to be overheard.
That is why we are heading for quantum cryptography, which perfectly minimizes the possibility of being overheard, and any eavesdrop can be detected.

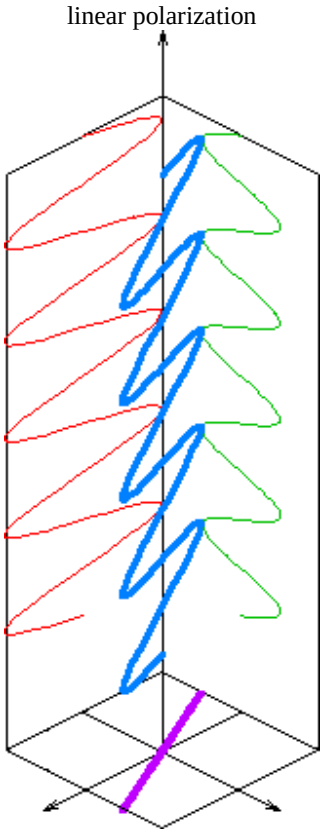
Theory

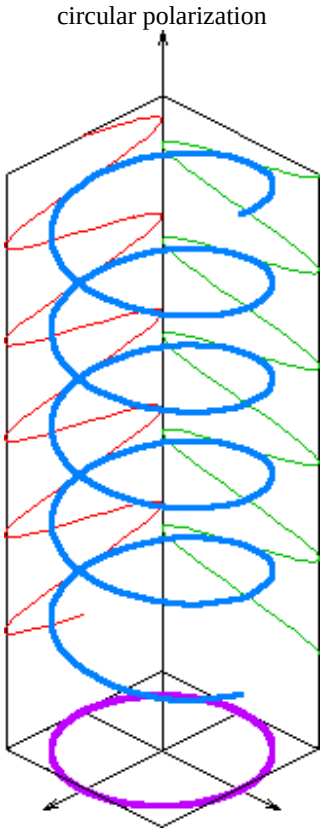
Quantum cryptography can be made possible by utilizing polarization of photon, which has the properties of both wave and particle.

Polarization of Photon
Under normal circumstances, a natural light wave can be described as a transverse wave superposed by many different kinds of wavelengths and polarizations.

A wave of this kind consists of enormous number of wavelengths, which can describe the data to be transferred. However they’re unsecured and can be easily hijacked.

Polarization helps to transform the wave of this kind to some specified shape by a polarizing filer and formed some *polarized light*. There are two different kinds of polarization, including Linear Polarization and Circular Polarization, whereas the wave’s photon motion will be in only one specified direction as controlled by the polarizing filter.





A polarizing filter in this case can be made from many different ways. One popular approach for visible light is to use a material called **Polaroid**, which is a special transparent polymer film.

Polaroid has selective absorption of the incoming light wave. Thus only the specified light wave can pass through the filter and this serve the purpose of polarizing.

Besides linear polarization, there is also circular polarization. When two linearly polarized waves with a quarter phase difference is superposed, the overall motion will appears like a rotating helix.

The circular polarization can be achieved by having a crystal (i.e. Calcite) that has different refraction indices for different direction of polarization. Hence by carefully adjusting the phase difference to a quarter-cycle, a circular polarization is made possible.

Uncertainty and Polarization

It seems still far away from our goal of quantum cryptography, which ensures the secure communication with the introduction of polarization. Hence we have to introduce the *principle of uncertainty* to light waves.

Classical Physics describe light as a kind of EM waves. But it's discovered that light can also be described as a transmission of photons instead (by the experiment of photoelectrons). This gives rise to the concept of **wave-particle duality of light**. Similar techniques are used in Quantum Mechanics to describe matter as well, but we'll concentrate only on light waves/photons here.

With the concept of wave-particle duality in mind, the appearance of a wave model can be

treated as the different intensity of photons in certain position, which is the probability of finding a photon in the given position. Hence whether you can find a photon or not is actually a *RANDOM* result!

The polarization of photon is again a result of probability. Say for example, we can find out that the probability of polarization is cos^2 (q). This shows that even the polarization of photon give rises to a problem of uncertainty.

The duality further implies that when we're to measure one of the properties of the photon (i.e. the circular polarization of it), we'll certainly disturb it. It's because of the uncertainty principle proved that *any attempt to measure one property of the wave and then resend it will disturb its other properties*. That is, although you're quite certain about one property of the photon, you're uncertain about the others and you can't 100% reproduce the same photon.

Defense Mechanism
With the introduction of uncertainty principle, secured communication using Quantum Cryptography can be made possible and practical in this sense.

A sender can send out a photon carrying a 1-bit of data passes through a polarizing filter via a optical fiber to the receiver, whereas the "1" or "0" carried by the photon is defined by the direction of linear polarization. The receiver then *randomly* applies another filter to the received photon and records it. After then, the receiver can verify the sequence of polarizing filter he/she has used with the sender and then get the right bits of data. If the sequence that they have used agrees with each other, the receiver has gotten the correct data.

In addition, the sender has to randomly apply the circular polarizing filter to either direction of polarization during the transmission so as to confuse the possible spy.

Whenever there's a middleman to spy the communication in the middle of the optical fiber, the middle-man have to measure the photon using either of the polarizing filter and then resend it using that filter. Since the middleman does not know the correct polarizing filter to use, like whether to use the circular one or linear one, hence **his/her involvement will disturb the signal** as explained above. So he can't simply fake the receiver/sender by re-encoding the data. This made his/her presence sensible to both the sender and receiver. Even the degree of spying can be measured by carefully comparing the selected bits of data sent/received by them.

Such defense is impossible using traditional ways of cryptography, since measuring the signal can be made invisible because of the lack of randomness. And that is the randomness of photons that ensured the security!

For example,

If the sequence of polarization used and data received/sent by sender and receiver is as follow:

Sender	1	0	1	1	1	1	1
Receiver	1	1	0	1	1	1	0

Whereas the gray boxes are which the Circular Polarizing filter is used, since they're not of correct sequence, this bit of data is rejected

After several times of correction, the sequences matched and thus the receiver gets the correct data.

It seems confusing to retransmit the data many times in order to retrieve the correct data, hence another approach called **entangled photons** are also used which is based on the pairing up of data between sender and receiver.

The data transmitted are thus the key that both the recipient and sender needed, and that is the way why Quantum Cryptography are often called **Quantum Key Distribution** (QKD) method.

Prospect

Quantum cryptography will revolutionise our communication. Everyone will be able to enjoy an unconditional message security. However, several problems are still to be overcome. Firstly, to bring about quantum cryptography, an independent network of optical fiber is needed. That means we will have to build an entirely new network solely for quantum cryptographic signals, which implies tremendous financial and engineering difficulties. Secondly, we need a device that can serve as a single photon source. Traditionally we can use the refraction method (or phase modulation) to filter out "unwanted" photons, but this is very hard to be done in the quantum level. Photons have a probability to exist after refraction, however slight is it. Optimistically it seems scientists and engineers are having considerable progress in these years, in not long a future will such a device be made.

Technology has a long history of being abused in warfare. A spear can hunt food or kill people. A nuclear warhead can threaten the evil or devastate the good. So by quantum cryptography, both security agencies and terrorists can enjoy perfect information security. We expect a fiercer tension between these two forces. Both sides will become heavily reliant to spying to get information by direct personal contact.

But if we combine quantum cryptography with digitising government and business services, media, copyrighted materials, online messaging, quantum computer, or even conscious artificial intelligence, interstellar communication, how well is quantum cryptography going to change our life? Nobody can be sure. Maybe some day, there will be robots chit-chatting quantum cryptographically, which gives no hint to us of what they are talking about; or we will confront with extraterrestrial civilisations which know this technology, and use this to play the toughest interstellar politics. Just nobody can be sure.

Appendix I - Reference

Wikipedia, Quantum Cryptography [*http://en.wikipedia.org/wiki/Quantum_cryptography*]
A Single-photon Server With Just One Atom
[*http://www.sciencedaily.com/releases/2007/03/070312111259.htm*]
Eavesdroppers Beware: Single Photon Emission Prepares Way For Quantum Cryptography
[*http://www.sciencedaily.com/releases/2000/12/001222072100.htm*]

Appendix II – Contribution of each author

Ng Yu Hang - Introduction + A brief history of cryptography
Tsoy Man Ching - Theory
Ying Ting Chung - Prospect

Ng Yu Hang
Tsoy Man Ching
peterpan795@gmail.com Ying Ting Chung