title: Ultimate Cryptography

author: Shinichiro Yamano

For thousands of years, people have sent letters in code not to be intercepted by third parties. Especially, kings and generals were well aware of the danger of the message being stolen by the enemy. Today, we use the Internet and can connect with people all over the world through e-mail or SNS. The scales of information exchange are different, more than ever, we need a secure way to transmit the information - *cryptography*.

Let's imagine that Alice wants to send a private message to Bob, but needs to avoid being eavesdropped by Eve. Cryptography is the method that prevents third parties from reading private messages. Using cryptography, a sender (Alice) and a receiver (Bob) can communicate securely without being overheard by Eve.

Since ancient times, kinds of cryptography have been considered. For example, Caesar cipher, named after a bright general officer said to have used the cryptography in wars, is the most famous one. The rule in a Caesar cipher is that Alice and Bob shift the letters by a predetermined number. For example, they promise that letters are shifted three places back in the alphabet, so "A" becomes "X" and "B" becomes "Y", and so on.

Today cryptography is widely used not just in war. Although we are rarely aware of it in our daily lives, most communication on the Internet is protected by cryptography. Think about when you shop at Amazon. Eve all over the world may try to get your credit card number.

In modern cryptography, the private message is scrambled by "key". The key is the random number sequence and Eve does not know. Refer to the previous online shopping

example, the key is shared between you and Amazon then your private information is transmitted securely. If Eve gets your “scrambled” card number, she cannot recover the original one without the key.

Therefore, cryptography can be considered the method to distribute the key to remote pairs. Nowadays the most commonly adopted cryptography is RSA. RSA is a clever way to distribute keys by using number theory. In this way, the security of RSA relies on the difficulty of the “factoring problem”. The basic idea is that calculating the product of two given prime numbers (a prime number is a natural number that is not a product of two smaller natural numbers, such as 2, 3, 5, 7, …) is relatively easy, but it is very hard to factorize a number into prime factors. Using the asymmetry of the difficulty, RSA guarantees security.

The history of cryptography is also the history of the battle against Eve. Eavesdropper Eve has attacked various cryptography. For now, RSA is safe but there is a possibility that it will be broken by supercomputers or quantum computers in the future. There are some reasons for the risk. First, the difficulty of prime factorization is not proved. Of course, many scientists believe it, but efficiency prime factorization algorithms have been researched and the performance of computers is improving every year. Second, quantum computers can solve the prime factorization problem fast. Some quantum computers are already running. In such a situation, RSA may not be secure forever. Is there no such thing as absolutely secure cryptography?

What I will introduce in this essay is "quantum cryptography", which security is guaranteed by quantum mechanics. In 1984 Charles H. Bennett and Gilles Brassard

proposed the first method for secure communication, which is now called BB84. Quantum mechanics describes microscopic phenomena and the behavior is very strange compared to what we see around us. By taking advantage of this property of quantum mechanics, we can create secure cryptography that is never broken.

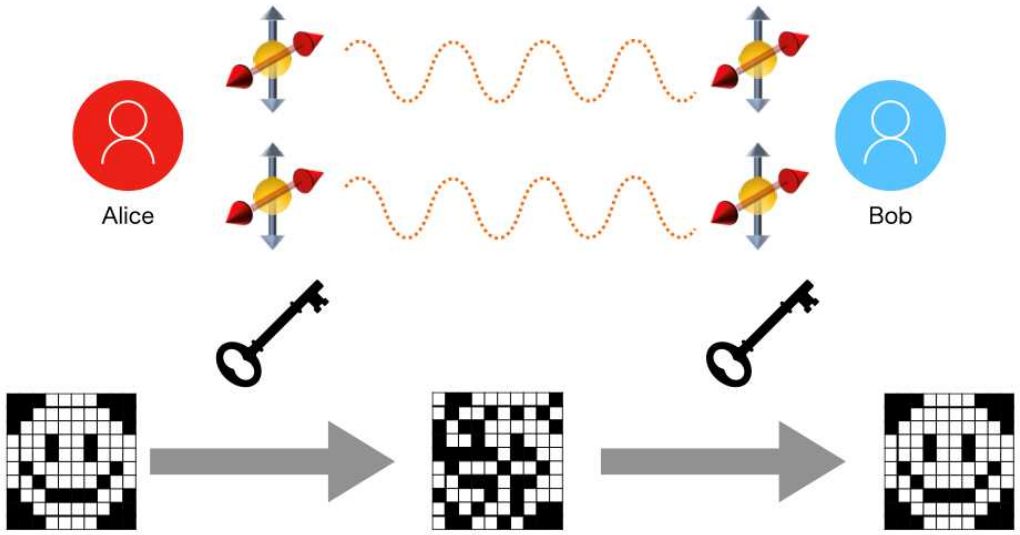
Before we get into the specifics of quantum cryptography, let me explain some important concepts. First, the "superposition". Let's consider photon. Photon is a particle of light. Light has a property called polarization, which is the direction of wave vibration. Our eyes cannot distinguish polarized light very well but in liquid-crystal display on TV or sunglasses, polarization is controlled. Polarization is divided into two directions: “Horizontal” and “Vertical”. Interestingly, in quantum mechanics, these two states can be superimposed. There are two types of superposition such as “Right-handed circular polarization” and “Left-handed circular polarization”. In its state, the wave rotates clockwise or counterclockwise. If we prepare “Right” state and measure “Horizontal” or “Vertical”, the result is absolutely random. That is, the probability of “Horizontal” and “Vertical” is the same 50 %. Surprisingly, no one can predict the outcome of the measurement. And so is “Left”.

Second, the "entanglement". One of the most famous entangled states is the Einstein Podolsky Rosen (EPR) pair. This pair illustrates the mysterious property of quantum mechanics. EPR pair is a combination of two photons and each photon is a superposition state. Curiously, if we measure one of the photon's polarization and get the outcome, the other photon's polarization is determined to be the same outcome instantly (even if it is from one end of the galaxy to the other!). The results are completely correlated. Let’s

think to measure the “Horizontal” or “Vertical” in two photons. If they are EPR pairs, the result is (“Horizontal”,” Horizontal”) or (“Vertical”, “Vertical”). In the same way, if measure the “Right” or “Left”, the result is (“Right”,” Right”) or (“Left”, “Left”).

The basics of quantum cryptography are explained below. Alice creating many EPR pairs and sending one of the photons to Bob. Then they measure the polarization of their own photons and obtain random results of (“Horizontal”, “Vertical” ) or (“Right” or “Left”). Alice and Bob share the same result so they can share a secure key. If Eve measures the polarization of the sent photon, the entanglement is broken. It causes non-correlated results (“Horizontal”, “Vertical”) and (“Right”, “Left”) to be generated and Alice and Bob can detect Eve’s eavesdropping. In this way, the theory of quantum cryptography makes full use of the magical properties of quantum mechanics to provide secure communication.

Other than the Amazon shopping example, there are so many opportunities for us to exchange information. As globalization progress, it is very important to guarantee communication security. Quantum cryptography can contribute to this task by using physics.


Alice
Bob