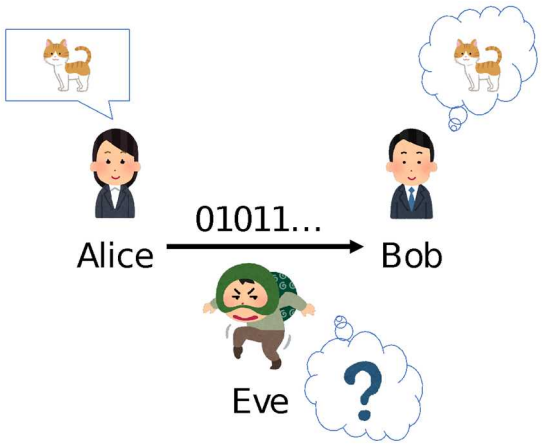
New type of secure communication in the era of quantum computers

Satoshi Yoshida (Department of Physics)

In recent years, the Internet has spread worldwide, and we can easily communicate many messages. Despite its convenience, it has a risk that malicious people can also access the messages. To prevent information leakage, we often encrypt the messages using some cryptosystem. A typical example is the Rivest-Shamir-Adleman (RSA) cryptosystem. It is believed that the RSA cryptosystem cannot be broken with a computer in current use, which is called a classical computer. On the other hand, with the recent development of quantum technology, the new type of computer is becoming a reality. It is called a quantum computer. In 1994, the American mathematician Peter Shor showed that a quantum computer could break the RSA cryptosystem. Therefore, it is necessary to use a new cryptosystem that cannot be solved even with a quantum computer when quantum computers are realized. For this purpose, various researchers on quantum information theory have investigated new cryptographic schemes.

First, let us consider the general theory of cryptography. Let Alice (sender) would like to send a private message to Bob (receiver). The communication from Alice to Bob may have been intercepted by an eavesdropper, Eve. The purpose of cryptography is to prevent message leakage to Eve. One of the oldest types of cryptography is called common key cryptosystem. The scheme is as follows. First, Alice and Bob share a number called a key in a safe manner. Then, Alice creates a ciphertext from the message and the key and sends it to Bob, who decrypts the original text using the key. Thus, even if Eve eavesdrops on Alice's communication to Bob, she would not get the original message unless she knew the number of the key. Common key cryptosystem has the advantage that it needs a small communication cost. Still, it has the disadvantage that it is usually challenging to share the key between Alice and Bob without Eve's eavesdropping.



On the other hand, there is a cryptosystem that guarantees security even if the key is leaked. It is called a public key cryptosystem. In this cryptosystem, the massage is

transmitted in the following procedure. First, Bob determines a public key and a secret key, and sends the public key to Alice. Then, Alice uses the public key to encrypt the message and sends the ciphertext to Bob. Finally, Bob uses the secret key to decrypt the ciphertext. Let us consider the case when it is very difficult to calculate the secret key from the public key. Then, even if Eve eavesdrops on the ciphertext and the public key, the original message would not be leaked because Eve cannot know the secret key. Therefore, this method has the merit of ensuring security even if the public key is leaked instead of incurring communication costs. The RSA cryptosystem is one of the standard public key cryptosystems. This cryptosystem requires solving a mathematical problem called the discrete logarithm problem to calculate the secret key from the public key. Researchers believe that this problem cannot be solved efficiently with a classical computer, so it is safe if Eve can only use a classical computer. However, quantum computers can efficiently solve this problem. Therefore, if Eve uses a quantum computer, she can break the RSA cryptography.

To solve this problem, researchers have investigated the public key cryptosystem in which encryption and decryption can be done efficiently with a classical computer, but the calculation of the secret key is difficult even with a quantum computer. Such a type of cryptography is called post-quantum cryptography. For instance, researchers believe that a mathematical problem called the lattice shortest vector problem cannot be solved efficiently even with a quantum computer. Therefore, the cryptography that requires the solution of the lattice shortest vector problem to calculate the secret key from the public key can be used to secure communication against eavesdropping with a quantum computer. Such a type of cryptography is called the lattice-based cryptosystem. Moreover, various other types of post-quantum cryptography have been proposed so far.

Post-quantum cryptography is a secure cryptography when Eve (eavesdropper) has a quantum computer, but Alice (sender) and Bob (receiver) have classical computers. If Alice and Bob have quantum computers, they can use another type of cryptography. As I explained in the second paragraph, if Alice and Bob can share a secure key, they can communicate messages securely using the key. It is known that they can share a secure key using quantum computers. The protocol is called quantum key distribution. One example is BB84, which utilizes the entanglement and the disturbance of measurement, both of which are unique properties of quantum theory. Then, even if Eve eavesdrops

on the key with these properties, Alice and Bob can know the leaked part of the key. Then, they can share a secure key by discarding the revealed portion of the key.

In summary, while the importance of cryptography is increasing due to the recent development of the Internet, the realization of quantum computers is approaching with the progress of quantum technology, which will make existing cryptographic schemes vulnerable. To solve this problem, researchers have proposed two types of cryptography, post-quantum cryptography and quantum key distribution. In other words, the recent development of the quantum computer has stimulated the study of cryptography, which has led to the discovery of new cryptosystems.