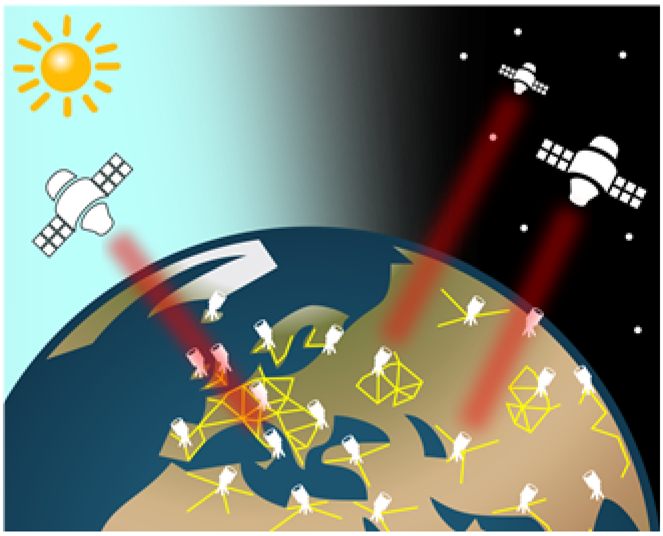
The art of communication



Ever made a call over the internet, sent an email, or transferred money to another account? The information age has revolutionized many aspects of our lives. With the introduction and expansion of computers and networks in the mid-20th century, a new world of possibilities is brought into perspective, and innovations expanded and eased the life of every one of us. This happened not only because of the fast growth of the global networks and miniaturizing computers, but also, we owe it to the advances in another field, cryptography. Transmitting information is not enough if that information contains sensitive data such as personal info, bank, health, etc. Data that needs to be known only by certain people or organizations.

Cryptography is a set of techniques that allows us to transmit data faithfully and securely between two or more parties in the presence of adversaries. Current cryptographic schemes, which are known as classical cryptography, are proved to be effective and efficient and their resilience against attacks performed with the most powerful computers is guaranteed. However, we are on the verge of the next technological breakthrough. Quantum computers, powered by peculiarities in quantum mechanics, can in fact demolish the current cryptographic techniques as they are very powerful and faster in performing certain tasks. Quantum computers are not ready yet, but this issue has brought much attention and scientists are preparing for the post-quantum era.

One approach, allowed by the laws of quantum mechanics, is called quantum cryptography.

In this short article, I am going to introduce new progress in realizing and implementing quantum cryptographical systems.

Classical vs. Quantum Cryptography

Cryptography is a set of techniques and mathematical algorithms to encrypt data, prior to storing or transmission, such that its content is safe against unwanted access. These techniques are mostly evolved based on computational hardness assumptions. In simple words, these mathematical algorithms are very hard, but not impossible, to be reversed without having access to extra information about the encrypted data. This makes trying an attack, in a reasonable time, impractical and pointless. This being said, the security stems from this type of algorithms highly depends on computational power.

Quantum cryptography, on the other hand, is an information-theoretic secure scheme. It means an adversary cannot break the encryption and access to data no matter how powerful he is. However, the practical realization of quantum cryptography in communication, known as *quantum key distribution (QKD)*, capable of supporting the vast amount of data we are transmitting every second is a hard task.

Why is it hard to do Quantum Key Distribution?

The difference between classical and quantum cryptography roots in the logic and idea behind them. In classical cryptography, data is encrypted at the transmitter and decryption happens upon receiving the data. This allows transmitting the encrypted information at arbitrary power. Imagine classical cryptography as a radio station with the only difference that the message broadcasted in every direction is encrypted. While it can be collected by anyone, only he who has access to the encryption key can decrypt it and actually read the data. Furthermore, to cover longer distances, it is only required to increase the signal power, or amplifies it on the way to the receiver, to overcome the loss that happens in transmission. For this, the distance does not pose a serious limitation on the rate at which data transmission can be done.

In quantum key distribution, on the other hand, information is encoded in the single quanta of light, called photons and the channel is called quantum channel. In order to prevent revealing the information by an adversary or tampering with the data, the intensity of signals is extremely low, and in the regime that laws of quantum mechanics hold. In this regime, quantum mechanics ensures the security of communication.

Transmission of such weak signals is challenging. Optical fibers that are common in classical communications is the first candidate for the quantum channel. Unfortunately, optical fibers suffer from loss which limits their practical application. QKD was successfully performed in a distance over 400 km, however, the rate is not yet sufficient for daily applications. The achievable rate is mainly limited by the loss and noise in the transmission line, the *quantum channel*, which leads to the loss of photons.

Free-space Quantum Communication

The barrier on the attainable rate in QKD put by loss in optical fibers can be overcome using the free-space channel as the quantum channel. In this case, photons are sent through free-space to the receiver. The main advantage of the free-space channel is the lower loss values that photons experience in free-space, although exploiting this type of channel for QKD introduces new challenges. Free-space QKD, and in particular, ground-satellite-ground channels opens the room to perform QKD in intercontinental distances, something that is not possible over fiber optics. QKD was performed between two ground stations establishing a free-space channel as well as ground-to-satellite in more than 1000 km. In our group, we are focused on performing QKD over free-space as well as fiber optics. We aimed to tackle the loss issue by establishing a free-space channel and realizing QKD over it. This work is the first integration of QKD and silicon-photonics, a highly promising approach in going towards compact, light, and low-power-consuming devices. The stability of the system and noise reduce the efficiency of a QKD system. In our group, we demonstrated a series of new techniques and performed a field-trial to put our system to test in a real-world situation.

Quantum key distribution is one of the first commercialized quantum technologies, yet, there is still much to do. The future global network is envisaged a world-wide coverage of quantum secure channels and to reach that goal, many obstacles need to be overcome.