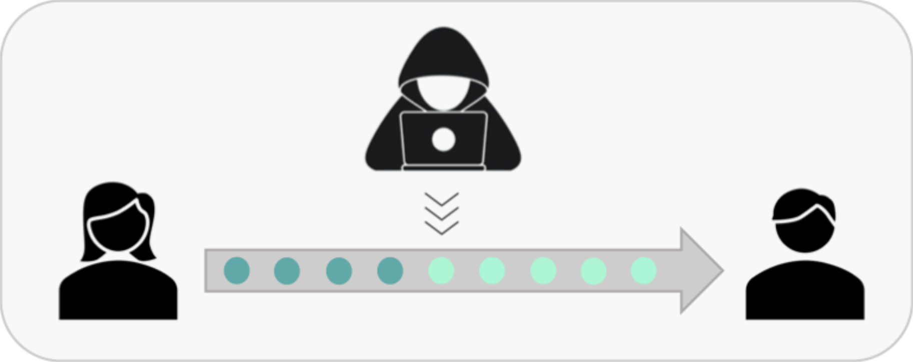
In a world of exciting technological possibilities, among the most significant are those enabled by quantum physics. Quantum physics is the theory of the microscopic world, it describes particles, atoms and molecules, and it is the underlying foundation of the digital age. For instance, it is thanks to this field of research that we have transistors on which today's mobile phones and computers are based, and lasers that are used in precision manufacturing. So far, almost all the technologies have exploited quantum physics only indirectly, and now, scientists are moving beyond it; they are working on directly controlling it to build new technologies. These technologies are set to have a profound impact on our society and economy by achieving things that are impossible or unthinkable with the current technologies. For example, they promise ultimately secure communications, ultrafast computation, precise sensing, precise timing information, and so forth.

Quantum communication is one of the most mature branches of quantum technologies, and it has the potential to completely change the field of cryptography. Cryptography is an indispensable technology in many applications where we require information security, such as financial transactions and the transmission of data containing sensitive personal information. Unfortunately, the current cryptographic systems are vulnerable to hacking because their security relies on the difficulty of solving certain mathematical problems, such as the prime factorisation of very large numbers. Problematically, this difficulty is not scientifically proven, it is merely assumed. This means that rapid technological advances or the arrival of new algorithms, including the construction of a large-scale quantum computer and the development of artificial intelligence, can completely compromise the security of our communications. At the moment, these technologies might sound like science fiction and give the impression that they will only become available in a very distant future. Nonetheless, experts estimate that by late 2030's, there will be quantum computers capable of breaking today's secure communications. In fact, intelligence agencies are already storing vast amounts of encrypted data in the hope that, in the future, they will be able to decrypt it and access important secret information. Therefore, the time to act is now. We have a unique opportunity to update our current communications systems before it's too late.

Quantum key distribution

Fortunately, and in contrast to conventional cryptography, quantum cryptography, or more specifically, quantum key distribution (QKD) promises to achieve unconditional security in data communication based on the laws of physics. More specifically, the security of QKD is based on the fact that it is not possible to copy the state of a quantum particle nor learn information about it without modifying it. Thus, information encoded in the state of a quantum particle, such as a photon of light, can be guaranteed to not have been observed if it arrives unperturbed from the sender to the receiver. What's more, the message transmitted will keep being secret forever irrespectively of the computational power and technologies that a hacker might possess in the future. Thus, QKD offers the strongest possible notion of security, and it often referred to as the Holy Grail of secure communications. In the last two decades, this field has developed significantly; now commercial QKD systems are available and QKD networks, including satellite-based QKD, have been deployed around the world. These tremendous achievements clearly demonstrate the potential of QKD to become a global technology.



If a hacker tries to eavesdrop on the communication channel, the state of the photons will be inevitably altered, causing transmission errors that signal her/his presence to the users.

Nonetheless, before QKD is widely adopted for securing our communications across the world there are a number of open challenges that need to be addressed. Some of these involve technical aspects, such as increasing the communication distance between users, improving the secure communication rate and reducing the costs of practical implementations. On the theoretical front, the most important challenge is to establish implementation security rather than the theoretical security. In theory, QKD has been mathematically shown to be unconditionally secure against any possible hacking attack. In doing so, security proofs typically assume idealised device models that have no noise or imperfections. Unfortunately, in practice, such idealised devices are not available, and by exploiting discrepancies between

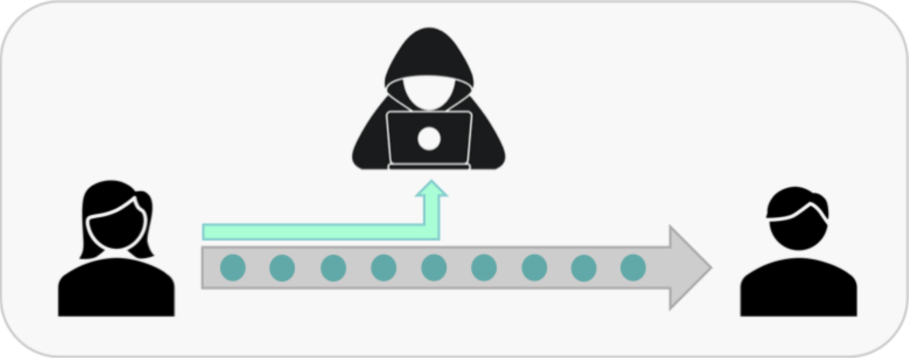
Quantum Communications for ALL (QCALL) is a European Innovative Training Network (project 675662) funded by the Marie Sklodowska Curie Call H2020-MSCA-ITN-2015.

the properties of ideal devices and those of practical devices hacking may be possible, compromising the security of QKD. In fact, several hacking attacks have been performed on experimental and commercial QKD systems, and they have succeeded. Therefore, to recover the unconditional security offered by QKD, it is crucial to develop security proofs that take into account device imperfections.

Usually, in a QKD protocol, there is a sending device that a sender uses to transmit secret information encoded in the states of photons, and a measurement device, which is possessed by the receiver to receive information. To remove the discrepancy between the idealised and practical devices and guarantee the security of this information, we need to develop better mathematical models that portray the real behaviour of the sending and measurement devices. By doing so, a practical implementation of this protocol is guaranteed to be secure even in the presence of imperfections, as long as they are sufficiently small. An important breakthrough in this direction was the introduction of *measurement-device-independent* (MDI) QKD. This is a QKD protocol that can offer perfect security even with arbitrarily flawed and completely untrusted detectors. In other words, we no longer need to take into account the imperfections of the measurement devices. Moreover, a variant of this protocol, called *twin-field* QKD, has been proposed recently, significantly improving its secure communication rate over long distances. Therefore, the missing step towards achieving implementation security is to secure the sending device. During my PhD, I have investigated and contributed to this issue, with the objective of achieving implementation security of QKD.

Securing the sending device

The most common imperfections in the sending device are state preparation flaws (SPFs), leakages of secret information from the user’s devices and correlations between the emitted light pulses. SPFs occur because real devices have a finite precision, hence the information encoded in the states of photons is slightly different from the information the sender wished to transmit. Also, leakages of information happen due to hacking attacks unknown to the users, or due to distortions in the emitted light pulses that depend on the information encoded. Finally, correlations between pulses take place because real devices hold in memory the secret information previously encoded, and inadvertently this information is passed on to the subsequent signals. All these imperfections open the door for a hacker to learn some secret information without being detected by the users.



Source imperfections allow a hacker to learn some secret information without altering the state of the photons, thus compromising the security of the QKD scheme.

Earlier attempts to incorporate source imperfections in security proofs of QKD have often resulted in very low secure communication rates. Recently, however, a *loss-tolerant* (LT) protocol was proposed, making QKD resistant to SPFs. That is, even when the encoding of the light pulses deviates significantly from the desired one, the secure communication rate is almost the same. Unfortunately, the LT protocol relies on the unrealistic assumption that there are no leakages of information from the users' devices nor pulse correlations, which is hard to guarantee in practical implementations of QKD.

In a work that I developed with my colleagues, we proposed a formalism to make the LT protocol more general by incorporating information leakages from the user's devices. In simple terms, we divided the emitted light pulses into a part that resembles perfect pulses emitted from idealised devices and another part that accounts for all the imperfections arising from using the actual devices. This allowed us to prove the security of QKD in the presence of multiple source imperfections.

The last step to secure the source is then to consider correlations between the emitted signals. To model such imperfection mathematically was believed to be the very hard because we need to deal with many pulses rather than a single pulse, which increases the complexity of the problem. For this reason, this imperfection has often been disregarded. Recently, we were able to develop a simple framework to incorporate this imperfection in security proofs of QKD. The key idea is to mathematically model the information encoded in the subsequent pulses as leakage of information. By doing so, we have been able to prove the security of QKD in the presence of pulse correlations between arbitrarily distant pulses.

Quantum Communications for ALL (QCALL) is a European Innovative Training Network (project 675662) funded by the Marie Sklodowska Curie Call H2020-MSCA-ITN-2015.

Importantly, this framework is compatible with the formalism that we created to deal with all the other imperfections.

Nonetheless, considering all these imperfections simultaneously inevitably reduces the secure communication rate of QKD. To counteract this effect, we have also proposed a new technique to prove the security of QKD that is more resilient to source imperfections. The main idea is to consider some reference states that are similar to the actual states, and use them as an intermediate step to prove the security of the actual protocol. Interestingly, the *reference technique* can reproduce previous analyses that deal with source imperfections, including our generalised LT protocol. However, its most striking feature is the easiness to incorporate source imperfections without severely compromising the secure communication rate of QKD.

As mentioned above, to achieve implementation security of QKD we need to take into account all imperfections in the sending and measurement devices. Fortunately, this can now be achieved by employing the security techniques we developed to deal with source imperfections together with an MDI-type QKD protocol, that assumes arbitrarily flawed detectors. In our latest work, using these ideas we have proposed a new protocol that is secure in the presence of any device imperfection. The only requirement is the characterisation of a single parameter that describes the quality of the source. Our protocol is the first QKD scheme proven to be secure in practical implementations. Notwithstanding, there are still theoretical and experimental challenges to finally establish implementation security. For instance, how to experimentally describe the quality of the sending device by a single parameter is still an open question. Moreover further improvements are needed in order to obtain higher secure communication rates and longer communication distances. Importantly, however, we now have a clear path for proving the security of QKD with arbitrarily flawed devices.

Quantum Communications for ALL (QCALL) is a European Innovative Training Network
(project 675662) funded by the Marie Sklodowska Curie Call H2020-MSCA-ITN-2015.