The importance of secure digital communications

One aspect of everyday life that has been revolutionised the most in modern times is our ability to communicate easily and nearly instantaneously from and to almost any part of the world. Listing all the aspects of life that have been affected by this revolution woul

d be a challenging task. But, just to mention a few, think about how we communicate with our friends and loved ones, on how we access financial services (ATMs, chip-based credit cards, online bank accounts), and about how we communicate in the work place (emails or direct messaging systems). In all these cases, digital communications have deeply changed the way we behave.

A good way to assess our increasing dependence on digital communication tools is by looking at the increase in the number of internet connected devices over the recent years (Fig. 1). Their number has increased dramatically over the last decade, reaching tens of billions.

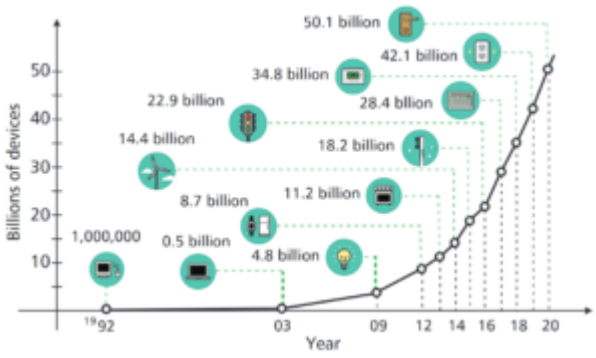

Fig. 1: Expected number of connected devices to the Internet. This chart is obtained from recent reports developed by both Cisco and Ericsson. Figure taken form this article.

As for any new technology, these new means of communication

generate new problems and risks. Among the most critical is the difficulty of keeping our digital communications private and confidential. Security is a crucial requirement for many of our communications. And it is for this reasons that over the past 60 years a lot of effort has been put into the development of cryptography, i.e. the set of techniques that allow us to transmit and store information securely. It is thanks to cryptography that nowadays we can have private digital communications.

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

What is Quantum Key Distribution and why do we need it

Most of today's digital communications are protected by *public-key cryptographic schemes*. The security of these is based upon two assumptions: there are certain mathematical problems that are very difficult (or almost impossible) to solve with *(1) current day technology* and *(2) mathematical knowledge*. These two assumptions looked extremely strong in late '70s when public-key cryptography was first introduced, but unfortunately today this is no longer the case. In the mid-90's it was demonstrated that, among other far-reaching capabilities, a powerful enough quantum computer could easily break the security of the currently deployed public-key cryptography schemes. This is a daunting prospect for the security

of our digital communications, especially given the recent impressive progress towards the construction of quantum computers.

The need for an alternative to the present cryptographic standards stimulated the research for a different approach to cryptography. One possible solution for this problem has been found in Quantum Key Distribution (QKD). The most interesting aspect of QKD is that its security is based upon a very different set of assumptions: the *correctness of the law of physics* (particularly quantum physics), and on the *unflawed physical implementation* of the devices used to set up the secure communication. There is a notable advantage with this approach: while advances in technology and limits to the mathematical knowledge are not under our control, the security of QKD is based upon something we have a more direct control of.

Limitations associated to QKD: cost, security and distance

Since its conception in 1984, the research around QKD advanced considerably, and reached remarkable results. We are now at a stage where this technology is practical enough to be implementable in real world scenarios and companies that sell ready-to-use QKD devices to the general public already exist.

Despite the recent progress in QKD development, a few limitations

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

associated with its implementation remain. The most relevant of which are:

1. the requirement of specifically designed hardware to perform QKD;
2. the cost of this hardware;
3. the security associated with its physical implementation;
4. the limited distance at which QKD operate run successfully.

Points 1 and 2 can probably be considered technical limitations. There is a lot of research addressing these issues, and much of it focuses on the miniaturisation of QKD devices into small form factors, compatible with scalable fabrication techniques and suitable for mass production. For more information on this argument, see the post by my colleague and fellow QCALL member, Innocenzo De Marco.

Points 3 and 4 are instead of a more fundamental nature.

The security of any QKD implementation relies on a perfect match between the theoretical model describing the system and its physical implementation. Therefore, in order to guarantee the perfect security of a system, two approaches are possible:

- One is to develop theoretical models that consider all the possible experimental flaws (see the work of my fellow QCALL member Margarida Pereira to get an insight on this type of research).
- The other one is to remove all the implementation flaws from the QKD device.

One of the most effective ways to implement this second approach happen to be the removal of the detectors from within the secure perimeter of the QKD system. This is the strategy used in Measurement Device Independent (or MDI) QKD protocols. These

types of protocol are considered more secure than the other QKD protocols because they are less prone to implementation security issues.

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

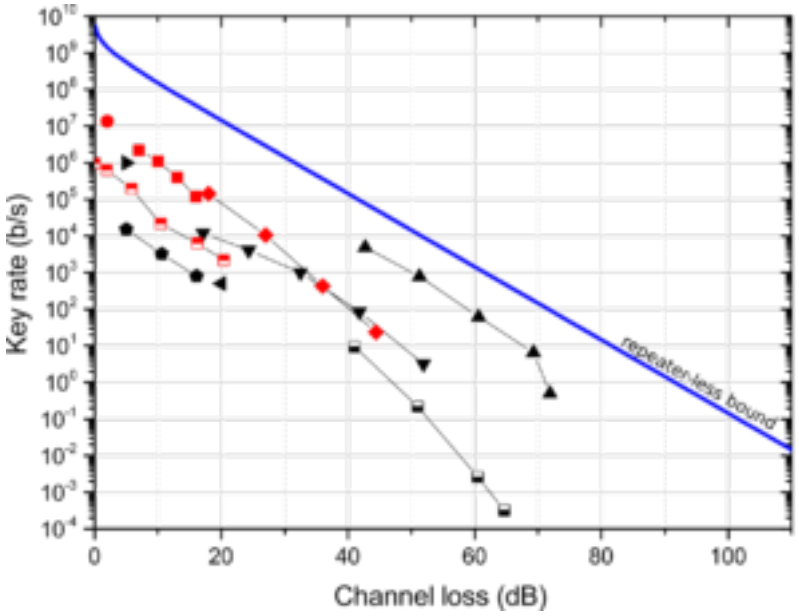

Fig. 2: Key rate obtained in state of the art QKD experiments, over channel loss. All the points in the graph lie below the thick blue line which is the PLOB bound.

The fourth and final limiting factor of QKD is the maximum distance at which it can operate successfully. This is fundamentally limited by the information carriers used in QKD, which are (in the ideal case) single photons. It can be proved that with the current technology there is a fundamental limit on the maximum key rate that is achievable over a certain channel loss. This limit is often referred as the repeaterless secret key capacity bound (or PLOB bound, from the name of the researchers that discovered it) and scales linearly with the channel loss (Fig. 2). In practice, the maximum distance covered by QKD communications reaches only a few hundreds of kilometres.

The focus of my research is demonstrating that it is possible to increase the maximum attenuation at which QKD can be performed, while maintaining the highest standard of security by removing the detectors from the secure perimeter of the setup.

Twin Field QKD: protocol concepts and advantages

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

At the beginning of 2018 a group of researchers at [Toshiba Research Europe Ltd.](Toshiba Research) published a paper that introduced a novel QKD protocol called Twin Field QKD (or simply TF-QKD). The protocol has several interesting features, the most remarkable of which is that it introduces a viable way to overcome the PLOB bound with currently available technology. This result is very relevant from a practical point of view because it means that there is now a way to extend the maximum transmission distance achievable by QKD.

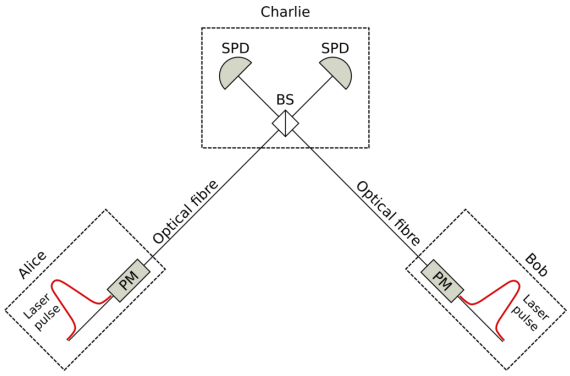

Fig 3: Simple schematic of the setup for TF-QKD. Inspired by figure in this article.

This result is possible thanks to a different way of encoding and retrieving the information in the quantum carriers used for the protocol. In TF-QKD the information is encoded in the phase of the optical pulses prepared by the two users that want to establish the secure communication, and the secret key is retrieved via a single photon interference measurement made by a user in the middle (see the simple schematic in Fig. 3). Another interesting aspect of TF-QKD is that it is also Measurement Device Independent, which means that it meets the strictest standards of security.

The advantages associated with this new encoding and detection strategy come at a price: TF-QKD introduces a series of new challenges that have to be faced for its implementation. The most difficult of which are:

1. The generation of twin optical fields from two space-separated laser sources;
2. The stabilisation of the channel used during the communication. This has to be stabilised to a new level of precision compared to other QKD protocols.

TF-QKD implementation

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

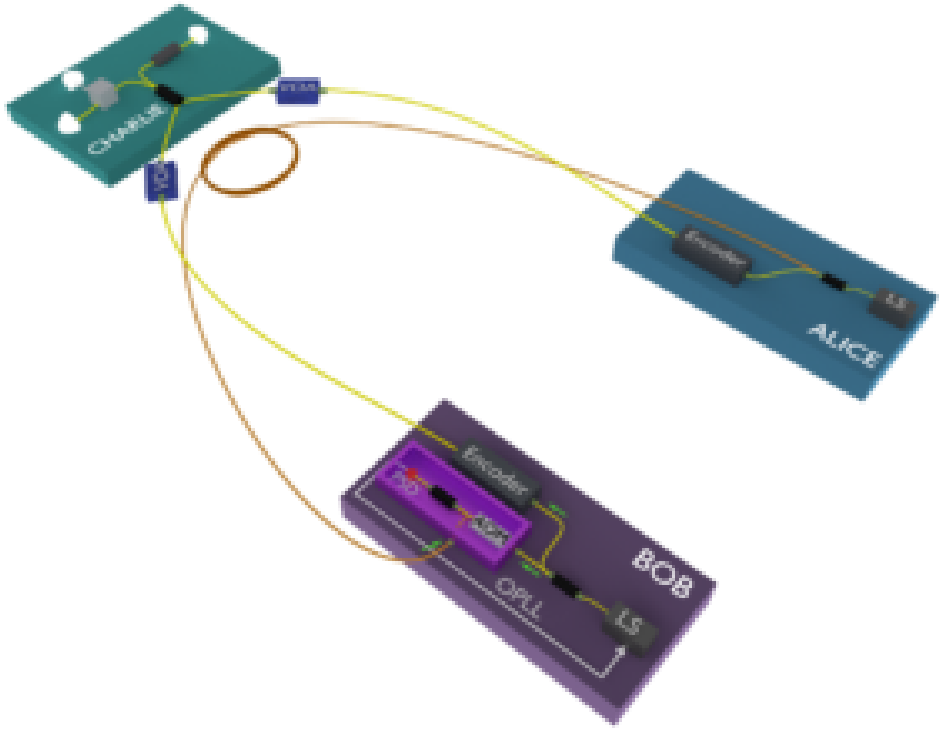

Fig. 4: Proof of principle TF-QKD experimental setup. Image courtesy of Mariella Minder.

The focus of my research within the QCALL network, has been to demonstrate the experimental feasibility of the TF-QKD protocol. For this purpose, together with my colleagues at Toshiba Research Europe Ltd., I developed the first TF-QKD setup, and proved that the protocol can indeed be used to overcome the PLOB bound.

The setup used for this task is shown in Fig. 4. It is important to notice that in this proof-of-principle experiment we simulated the channel attenuation associated with a long communication channel by means of Variable Optical Attenuators (VOAs, optical devices that set a chosen attenuation over an optical channel). This enabled us to execute the experiment at extremely high channel attenuations, without having to worry too much about the phase fluctuations that would have been introduced by long optical fibers.

The elements of novelty in this setup, compared to other QKD implementations, are the frequency distribution system (represented by the brighter purple box in Fig 4), and the system used for phase stabilisation. More information on these are given below.

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 frequency distribution system: Optical Phase-Locked Loop

A technique developed in classical optical communications was borrowed for the optical frequency distribution. With this technique, called Optical Phase Locked Loop (or OPLL), it is possible to force two lasers to emit at the same optical frequency. This is done by locking the interference beating between two lasers to a target frequency through a PID controller connected to an actuator. See Fig. 5 for a more detailed schematic of the OPLL implementation in our setup.

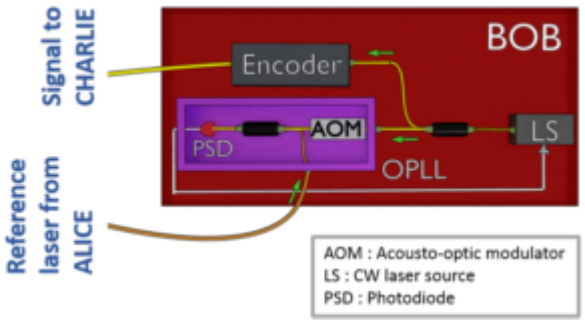

Fig. 5: Schematic of the OPLL setup.

The quantum channel stabilisation

Since in TF-QKD the information that the users want to communicate is associated to the phase of optical that they prepare, it is fundamental to keep track of the phase fluctuations between the two users. In this experiment we have accomplished this by stabilizing the phase of the quantum channel to a fixed and known value. To achieve this, some reference pulses were interleaved into the phase encoded pattern, and a phase feedback system was developed. The phase feedback system was composed of a PID controller and a phase modulator.

Results and outlook

With this setup we were able to execute TF-QKD at different channel attenuations. We performed the protocol at several attenuation levels, spaced roughly by 10 dB, and extracted a secret key that could be used for a secure digital communication. The results of this experiment are shown in Fig. 6 (the points in the plot), alongside the simulation curves. Our experimental results align very well with the values predicted by the simulations.

After its introduction, a lot of interest arose around TF-QKD, and several protocol variants have been proposed since then. The different colours for the points in Fig. 6 represent different TF-QKD protocol variants tested with this experiment. Our experimental setup had

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 flexibility to implement 3 variants in total: the original TF-QKD protocol (in red in the graph), the Send-Not-Send TF-QKD protocol (blue points in the graph), and the CAL TF-QKD protocol (yellow point in the graph).

It is remarkable that for all these protocols we managed to obtain a positive key rate above the PLOB bound, overcoming experimentally the repeaterless secret capacity bound for the first time ever. We also note that for the original and the SNS protocols we achieved a positive key rate at unprecedentedly high channel attenuations, that would be equivalent to the losses introduced by more than 500 km of ultra-low loss fiber.

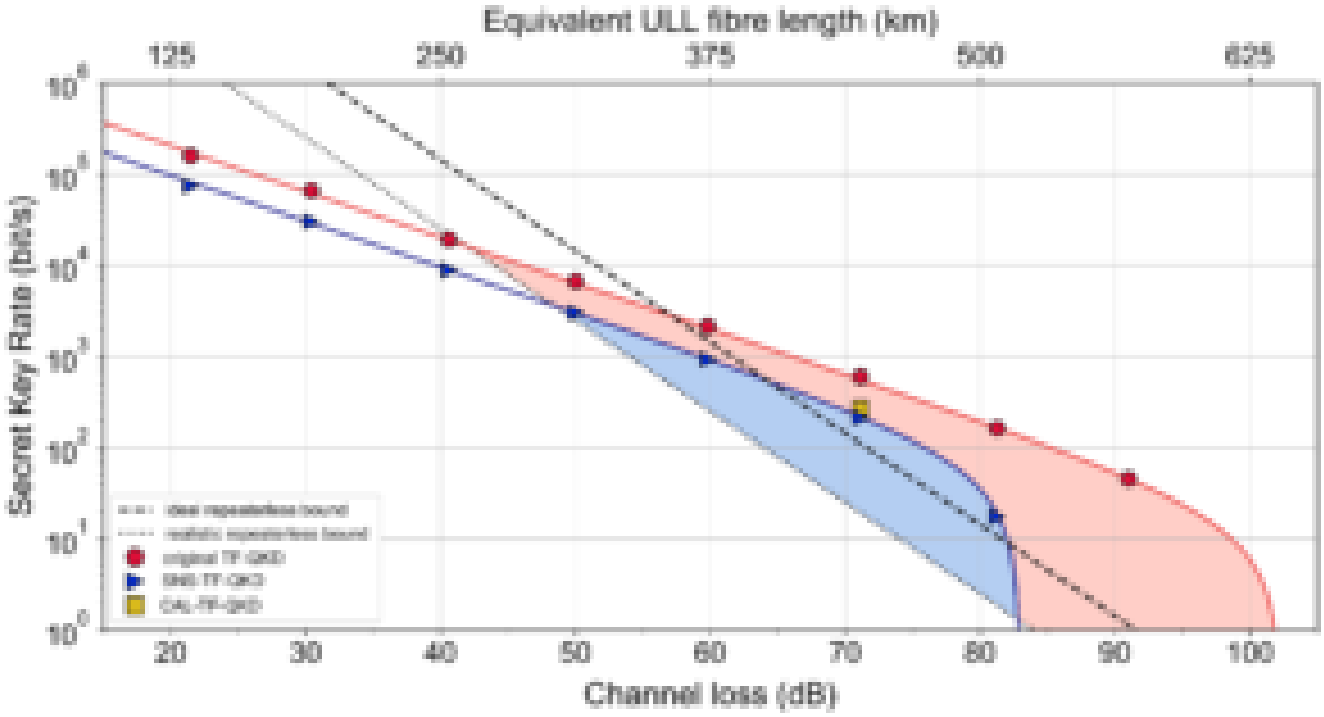

Fig 6: Key rate generated by our TF-QKD system art different attenuations, for various TF-QKD variants.

This experiment was the first demonstration of the feasibility of the TF-QKD protocol, and the first experimental evidence that it is possible to overcome the secret key capacity bound with current day technology. This experiment can be considered the first realisation of an effective quantum repeater, as suggested by a recent review on the advances in quantum cryptography.

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

Mirko Pittaluga

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