Introduction

As we live in the era of internet, online shopping/banking, it is basically an everyday task to enter our passwords and credit card data on different websites. The encryption (so that a malicious third party cannot infer our actual data) of this sensitive data that we send throughout the internet is based on the fact that some mathematical problems are extremely difficult to tackle with our current computers. Specifically, it is practically impossible to factorize very large numbers. However, in the other direction, if a factor is known then it is really easy to determine its cofactor. This asymmetry in the difficulties can be converted into the most widely used public key cryptosystems, which is called RSA, after its inventors.

The natural (quite disturbing) question arises whether this kind of cryptosystem is going to stay secure in the future knowing how fast technology is advancing. It is even scarier if one considers the progress on the development of quantum computers. With quantum computers the task of factorizing large numbers becomes exponentially faster with the so-called Shor's algorithm.

Solution: Quantum key distribution (QKD)

In 1984, with the appearance of the famous BB84 protocol, it became clear that quantum mechanics can be used to fight against the threat that comes with future quantum computers. With encoding information into quantum systems and performing quantum mesurements on them can in principle be used to create a secret key between two distant parties (usually called Alice and Bob). This method is called quantum key distibution (QKD), which can achieve an identical, random and secret bit string (consting of 0-s and 1-s) between Alice and Bob via the most fundamental laws of quantum physics thus security is no longer based on computational assumptions (opposed to RSA). This resource then can later be used to encrypt the messages with the so-called one-time-pad (OTP), that is, Alice adds the key to her message (also consisting of 0-s and 1-s) bitwise modulo 2 (which basically means that 1+1=0). Thus Bob can decrypt the encrypted message by adding the same key bitwise to the encrypted message.

The security is based on the no-cloning theorem, stating that it is impossible for an eavesdropper to make perfect copies of arbitrary quantum states. Note that for classical bits

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

copying is possible, therefore this is an apparent advantage that quantum mechanics offers.

Some difficulties of QKD: Repeaterless bound and source imperfections

The idea of QKD is relatively simple and elegant but in order to be a mature technology that can be deployed world-wide for everyday use, it has to overcome some limitations. In my research I try to come up with solutions in order to improve the performance of different QKD protocols, or at least to identify their limitations. The performance of a QKD protocol is characterized by its secret key rate, that is the number of secret key bits a certain protocol can generate per transmitted signal.

Repeaterless bound

One important theoretical limitation on the performance of point-to-point (when the parties are directly connected via a quantum channel that can be for example an optical fiber, or even free space) QKD protocols is the so-called repeaterless bound. This bound for the achievable secret key rate is exponentially decreasing with the distance for long distances as it can be seen in Figure 1 (note the logarithmic scaling). This is caused by the fact that the probability that a photon survives travelling through the optical fiber connecting the parties decreases exponentially with the length of the fiber, this probability is called channel loss. As this is a very stringent limitation, it has to be overcome if long distances have to be covered by point-to-point QKD and one desires to have a reasonable secret key rate.

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

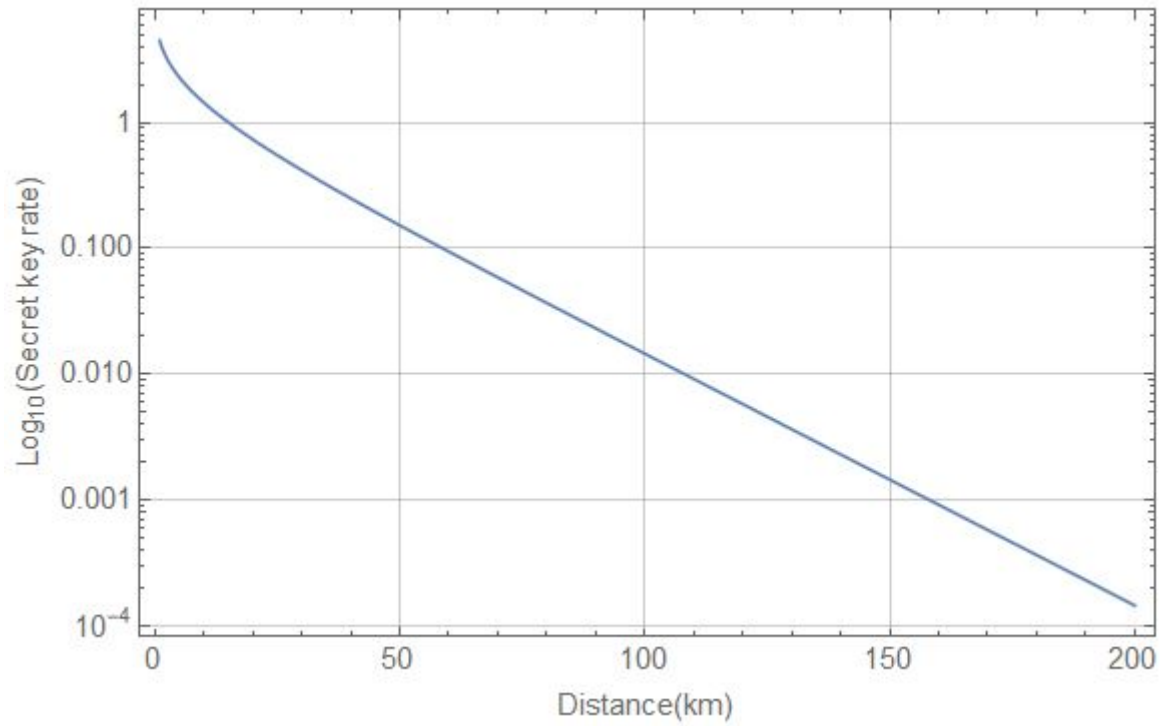

Figure 1. The repeaterless bound

It is clear that intermediate nodes (repeater stations) between the parties have to be introduced to go beyond the repeaterless bound so that the photons do not have to cover the full distance between the parties (but only the half of it) to be useful for generating a secret key bit. If the channel loss corresponding to an optical fiber of length L is t then the channel loss for the half of the fiber is the square root of t.

The most recent solution to surpass the repeaterless bound is the so-called twin-field QKD (for more information see the spotlight article by ESR Mirko Pittaluga).

In my research, however, I focused on other types of approaches in order to overcome the repeaterless bound. The first one is a kind of adaptive QKD protocol, that is schematically depicted in Figure 2. The main point here is that the key generation process (denoted by BM in Figure 2) is only performed between successfully arriving photons (sccessful arrival is checked by the QND module), therefore, the key rate increases as every key generation trial is between actual signals that reached the middle station C. Otherwise it would be possible that a photon is lost on one side, which is not sufficient for establishing correlation 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 parties.

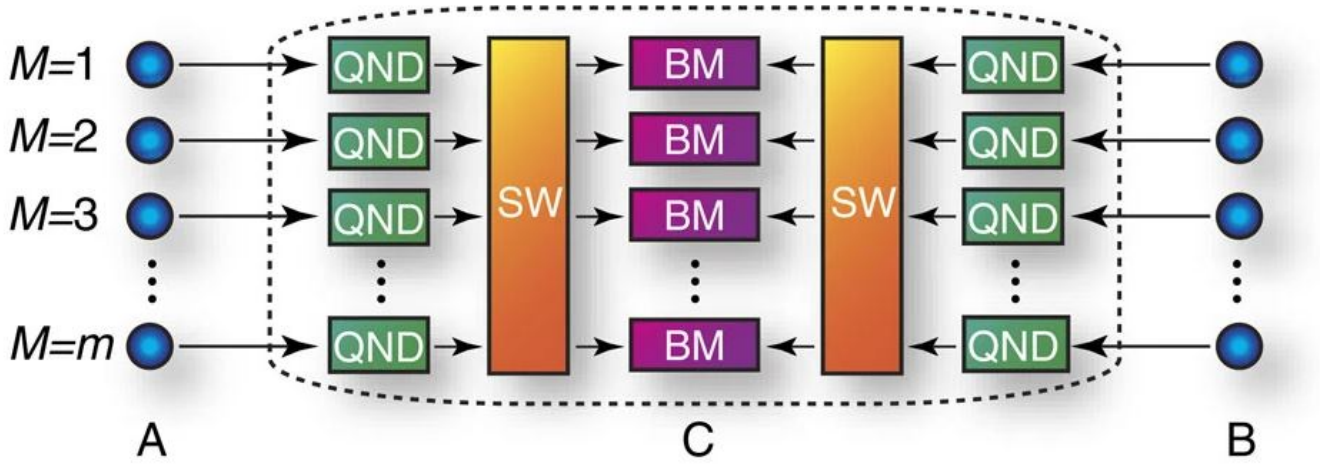

Figure 2. The schematic layout of the adaptive QKD protocol. Figure taken from this paper.

For the original proposal in Figure 2, idealized devices were assumed (e.g., perfect single-photon sources) and the authors showed that it is possible to overcome the repeaterless bound with this protocol.

In our work, we calculated the secret key rate of the original protocol if the idealized single-photon sources are substituted by the practical (and widely available) parametric down-conversion (PDC) sources (which sometimes emit two or more photons pairs). We found that with PDC sources the protocol is no longer capable of overcoming the repeaterless bound. Thus the performance is very sensitive to the imperfections of the devices.

In, we investigated the performance of the protocol depicted in Figure 3, which is very similar to the protocol from Figure 2, but it is without QND modules and instead so-called quantum memories (QM) are applied in order to overcome the repeaterless bound. The QMs are able to store a quantum signal, therefore a quantum signal on one side can patiently wait until the signal from the other side successfully arrives and then a BM module carries out secret key generation. The working principle is the same as before, making sure that the key generation is only performed between actual signals.

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

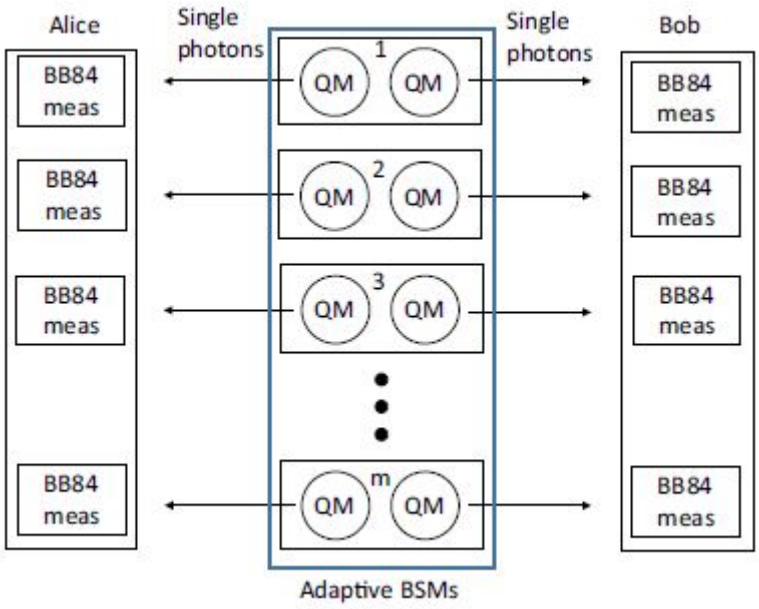

Figure 3. Schematic layout of the Quantum memory assisted protocol.

We characterized the necessary experimental parameters for the protocol to beat the repeaterless bound as a function of the applied QM pairs. The most important parameter of the devices is the dephasing time constant of the QMs, which describes how fast the stored quantum state changes over time (so higher quality memories have higher dephasing time constant as this depahsing leads to errors). We found that the requirement for the dephasing time constant of the QMs can be relaxed significantly if the number of QM pairs increases. But even with a lots of memory pairs it is far from trivial to overcome the repeaterless bound with current technology using this QM based protocol.

Source imperfections

The ideal information carriers for QKD protocols would be single-photons as a single-photon is a quantum mechanical object that cannot be copied due to the no-cloning theorem, however, in practice it is really challenging to implement on-demand perfect single-photon sources. Therefore, in the lab, the desired single-photon sources are approximated by dim laser pulses, but sometimes these pulses contain more than one photon. Whenever this happens, the information is not encoded only into a single entity but it is inherently duplicated so an eavesdropper Eve (who is only limited by the laws of quantum physics) can take one photon

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

out of the two or more photons and keep it to herself thus she will have the same information carrier as Bob so the security of the protocol is compromised. This is called the infamous photon number splitting (PNS) attack. This means that additional techniques have to be applied to avoid the possibility of such an attack.

A simple protocol to fight against the PNS attack is the coherent-one-way (COW) protocol since it encodes the information coherently between different laser pulses and at the receiving end Bob checks that such coherence is kept. The PNS attack breaks this coherence, so the COW protocol should be able to detect it. Long distance experiments and even commercialized products have appeared based on this scheme. We show that, despite of its popularity, the COW scheme is not robust against other type of attacks.

Here, we designed an attack against the COW scheme, proving that all implementations of this protocol reported so far in the scientific literature are actually insecure. The attack is based on a technique called unambiguous state discrimination (USD). With USD it is possible to discriminate the different quantum signals (that Alice sends) without misidentifying them. This comes at the cost of sometimes obtaining an inconclusive result. If Eve applies this strategy in a clever way, she can remain undetected for the parties (she will not break the coherence between the signals) since she never makes a mistake in identifying the states. In this attack she measures all the quantum signals coming from Alice to Bob and based on her measurement results she prepares new signals that she sends to Bob.

The evaluation of our attack appears in Figure 4, where one can see that the attack can provide better values for both of the monitored quantities (quantum bit error rate and the visibility that describes how the adjacent coherent laser pulses by Alice interfere with each other) than what can be achieved in the actual experiment, which makes it insecure.

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

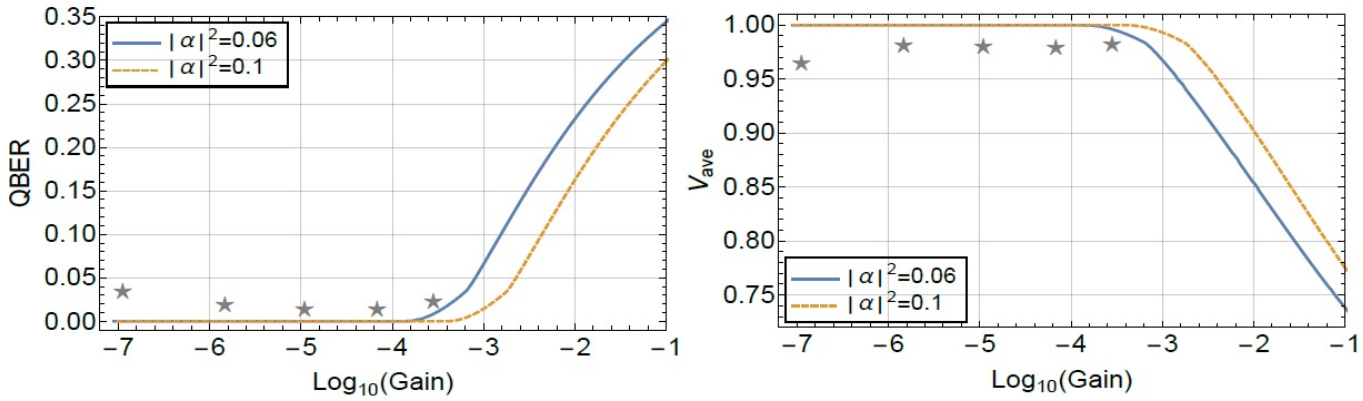

Figure 4. The stars represent the values achieved in the experiment, the curves represent the performance of our attack.The two different lines correspond to the two different intensity settings that Alice uses. The smaller gain values basically mean longer distances.

The most important consequence of our attack is that we showed that the secret key rate of the COW protocol is proportional to at most the square of the channel loss between the parties so its performance is much worse than what had been thought before.

Conclusions

We have seen that improving the performance of QKD protocols is an important task towards building a global quantum communication infrastructure for communications, which could be the remedy for the threat on the secrecy of our communications by future quantum computers. But at the same time it is a challenging task due to, for example, the difficulties attributed to theoretical limitations like the repeaterless bound or to the fact that the real-life devices used in an implementation are always imperfect. We have also seen that the popular COW protocol is not an appropriate candidate for long distance QKD.

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