Contribution ID: **38** Type: **Talk**

Fully passive quantum key distribution

Monday 29 May 2023 10:20 (30 minutes)

In recent years, quantum key distribution (QKD) has become a fully fledged application of quantum information science, and QKD services are being supplied by different companies/institutions around the world. However, the practical security of QKD is not well-established yet, mainly due to the difficulty of guaranteeing that real QKD implementations stick to the assumptions and models on which theoretical security proofs rely.

A particularly conflictive assumption present in most QKD security proofs is that no information is undesirably leaked outside the users'locations. In fact, optical QKD systems typically rely on the use of active modulators to encode the key information, and these modulators may be a source of side-channels in different ways. For instance, an eavesdropper may actively tamper with a QKD module to gain information about the protocol settings or, more simply, the information can be inadvertently encoded in undesired degrees of freedom.

A candidate solution to overcome this problem is to consider passive (rather than active) state preparation, which rules out all possible modulator side-channels by avoiding the use of active modulation of any kind. Precisely, a passive QKD transmitter generates the quantum states prescribed by a QKD protocol at random, combining a fixed quantum mechanism and a post-selection step. Putting the security upgrade aside, getting rid of all actively driven elements could be very appealing for QKD in practice, because it may allow to boost the frequency of operation of QKD systems while reducing the complexity (and thereby the cost) of QKD infrastructures. Needless to say, this would entail an advantage in many practical situations, for instance, when it comes to deploying QKD on a satellite. Notably though, these advantages come at the price of decreasing the key generation rate because of two main reasons. On the one hand, in a passive transmitter, additional sifting is required to discard those protocol rounds where the randomly generated settings do not lie in certain acceptance intervals. On the other hand, the quantum states post-selected in a passive transmitter are in a mixed polarization state. This represents an inherent source of noise not present in the active case, where one typically considers perfectly prepared pure states.

In a recent collaboration, we presented the first linear optics scheme suitable for fully passive QKD, and analyzed its expected performance within two sharply different approaches for polarization encoding and secret-key-rate estimation. However, these analyses addressed the asymptotic limit of infinite signals, and in both cases the distillable key rate was limited by the inherent noise of the mixed polarization states. Here, we report on a novel parameter estimation technique that surpasses this limitation —in so reaching tighter bounds on the secret key rate— and address the practical scenario where a finite number of signals is exchanged. Furthermore, the developed techniques for the estimation of the secret key parameters might be of independent interest for the field of quantum cryptography.

Author: ZAPATERO, Víctor (Vigo Quantum Communication Center)

Co-author: Prof. CURTY, Marcos (Vigo Quantum Communication Center)

Presenter: ZAPATERO, Víctor (Vigo Quantum Communication Center)

Session Classification: Session 4.1