6
Conclusions and future developments

The field of quantum communications is losing its status of just "cool" physics and ground-breaking experiments to having real-world practical applications, and thus starting to integrate within the field of engineering. This is just one more example of fields becoming ever more multi-disciplinary. This field-merging trend is likely to continue for a long time and it is one more way of demonstrating that science has no boundaries.

For many engineers, quantum physics is something very far away from regular day-to-day activity, only mentioned at a general physics course as part of most elementary curricula. For others, some deeper knowledge is required to work in fields such as electronics or optics. Still for most engineers, to deal with individual quanta used to sound like work that only physicists would do. This statement could not sound more wrong in the age of miniaturization we are moving towards. Everyday devices shrink, computers get more powerful and technology gets more widespread use. With this comes a price: As components features get smaller and smaller the semi-classical physics that govern their behavior, and which has served us so well since the invention of the transistor, may no longer be valid. A full quantum picture is needed, and many theoretical aspects are already solved. We already know many different ways of how quantum information and processing works, and which operations it can perform. Many experiments have been done with successful and important results, however integration within systems outside of the lab are still lacking. Until a few years ago there had been few trials performed in real-world conditions.

This picture is steadily changing, however, as the commercial applications begin to see a need to use quantum information as well as its classical counterpart. The most clear example of this is quantum key distribution since digital security gets many headlines in the news nowadays. QKD is not yet ready for widespread use, but when we compare the latest research results compared to 10-15 years ago we can see how much it has advanced. It is difficult to predict where we will be 15 years from now in QKD, but we can only expect to see its use more diffused.

This thesis, written in an electrical engineering department, is one more attempt to bridge the worlds of engineering and experimental physics. As such, it was written mostly with an engineering point of view focusing on how the experiments were done. In Chapter 2 a brief introduction to quantum communications was given, with the aim of aiding newcomers to understanding the engineering problems of experimental quantum communications. It is not meant as a self-contained introduction, and references are given as appropriate. Readers seeking to know more are encouraged to look into those.

Chapter 3 contains the main results of the two experiments the author took part in during his stay at KTH in Stockholm. The first experiment used a narrowband non-degenerate entangled photon pair source, with the signal photon detected locally by Alice, and the idler sent to Bob over 27 km of SMF-28 optical fiber. The synchronization signal is sent through the same fiber using wavelength multiplexing with a channel separation of only 0.8 nm, making it compatible with optical networks. The visibility results achieved show that QKD is possible with such a setup. The other experiment involved the construction and characterization of a non-degenerate heralded single-photon source, to be used in a QKD experiment with the decoy state method implemented. This was the first time decoy states were used experimentally with a source based on SPDC. Results matched the theoretical predictions, and in spite of our lossy setup, a successful key exchange was achieved with satisfactory results.

In Chapter 4 the results from the two main experiments performed at PUC-Rio after the author's return from Stockholm. The first is a study of Raman induced noise generated from a classical channel onto a quantum channel, both present in the same optical fiber. This study was motivated when the setup for the polarization control experiment presented in Chapter 5 was being initally tested. The study showed that transmission of classical and quantum channels simultaneous in the same fiber is non-trivial, but possible with current technology. Solutions to minimize the impact of Raman noise, such as narrower filters, and low transmitted powers were suggested. The other experiment was based on an idea that came up one day on a lab discussion on how to generate truly random numbers. The protocol we designed can generate truly random numbers independently of the rate the system works on, and is secure against Eve's attacks. A proof-of-principle experiment was performed demonstrating the validity of the idea.

Finally Chapter 5 presented an experiment done in collaboration with the GAP-Optique, from the University of Geneva. The prototype of the automatic polarization control system was assembled and tested at PUC-Rio, and the quantum key exchange done at Geneva. Results are very promising, showing that it is possible to transmit secure keys with polarization-encoded qubits using our prototype even in the presence of fast polarization changes applied to the single-photons via a polarization scrambler.

The results presented in this work leave a few doors open. The polarization control system we developed can be used in future experiments requiring polarization encoding in optical fibers, such as long-distance Bell-state measurements. It is also possible to do a polarization encoded key exchange in an installed fiber cable subjected to strong polarization fluctuations such as an aerial cable. It also is worthwhile to study the Raman noise issue further, performing simulations and measurements with fiber spools of different lengths, as well as characterizing other non-linear effects. Finally one other route to pursue is a theoretical analysis of the security of the random number generation protocol.