quantum cryptography

armando pinto[1]
nuno silva[1]
nelson muga[2,3]
álvaro almeida[3]
steven carneiro[2]
luís martins[2,3]
gil fernandes[3]
manfred niehus[3,4]
paulo andré[2,3]
rogério nogueira[2,5]
joão pinto[6]

1 department of electronics, telecommunications and informatics & instituto de telecommunicações (IT), university of aveiro
2 department of physics, university of aveiro
3 instituto de telecommunicações (IT)
4 lisbon higher engineering institute (ISEL)
5 nokia siemens networks portugal, s.a.
6 department of physics & I3N, university of aveiro

In this project, we have been engineering secure fiber-optic communication systems based on quantum cryptography. Instead of being based on unproven lack of computational power, like traditional cryptographic protocols, quantum cryptographic protocols rely on fundamental laws of nature to guarantee that any attempt to hack into a communication system cannot go undetected.

In the framework of the project "*QuantPrivTel – Quantum Private Telecommunications*", we succeeded in generating, transmiting and detecting single and entangled photons. Single photons are elementary particles that follow the rules of quantum physics.

After coding information in the photons' polarization, any attempt to extract the information using a wrong basis is going to produce a random result, i.e. noise. Entangled photon pairs are pairs of elementary particles that exhibit non-classical correlation, which makes any attempt to extract the information in one photon noticeable in the other photon of the pair.

To generate a stream of single-photon pulses, we are using the stimulated four-wave mixing effect in optical fibers. The four-wave mixing is a Kerr nonlinear phenomenon that occurs when photons' from one or more waves are annihilated and new photons are created at different optical frequencies preserving the aggregate momentum and energy. We are able to control the number of photons per pulse on average by manipulating the efficiency of the four-wave mixing process.

We are using the spontaneous four-wave mixing in optical fibers to generate entangled photon pairs. We have been exploring the momentum and energy conservation of the generated photon-pair to manipulate the photon quantum states. We have made coincident measurements and with these measurements we are able to assess the quality of the photon-pair generated, namely the degree of entanglement. We observe that the spontaneous Raman scattering is a major source of non-correlated photons. We found that in a single-pump configuration, photon-pairs can be created with polarization either parallel or orthogonal to the pump. In a dual-pump configuration, we found that by manipulating the optical power of each pump we can improve the quality of the generated photon-pair. We also found that orthogonally polarized pumps can generate photon-pairs with a high degree of entanglement.