Quantum Key Distribution (QKD) is a protocol which is provably secure, by which private key bits can be created between two parties. The security of QKD is conditioned only on the laws of physics being correct! Since information is coded as a quantum state of a particle - light polarization, electron spin, etc - an eavesdropper cannot gain any information from states sent from A to B without disturbing them and having A and B notice.

In practice, A and B must use noisy channels to communicate. When photons are sent down a fiber optic and coded in phase, noise resulting from the environment can disturb their state mimicking an eavesdropper, rendering the channel insecure.

In 2004, we realized a table top QKD protocol with error filtration using a single-photon detector.

Principle of the Set-up

A encodes her information in time bins using very weak coherent states, a 50/50 coupler and a phase modulator. She uses two more couplers to encode the filtration.

The information travels down four noisy channels and is then decoded with two Mach-Zehnder interferometers such that the erroneous information is discarded.

Finally, B measures the information with a 50/50 coupler, a phase modulator and a single-photon detector.

Experimental Results

This process enables one to perform secure QKD in a regime which would, without filtration, be insecure.


Contact: Serge Massar - Physique théorique CP 225, Université libre de Bruxelles, B-1050 Bruxelles, Belgique - smassar@ulb.ac.be