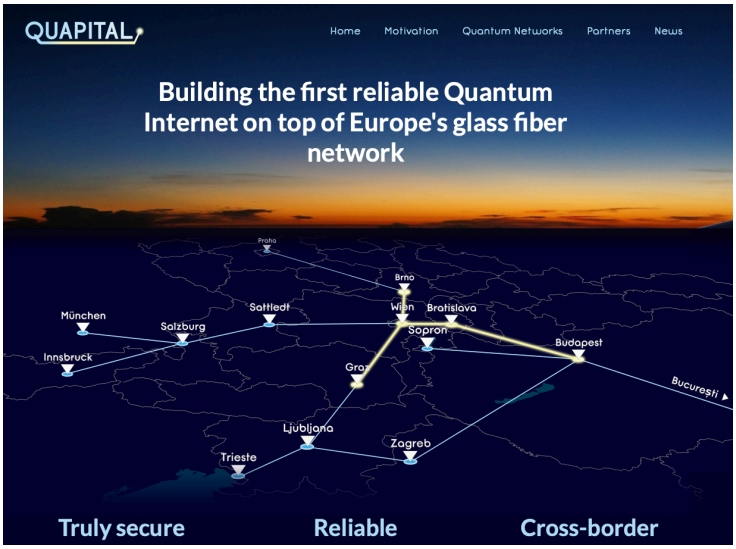
Secure Quantum Communication

Public key cryptography is widely used by banks to perform secure money transfers, or over the internet for securing website access. The security of public key cryptography relies on the difficulty of realizing an efficient algorithm to “crack” the communication. These protocols are not, however, unconditionally secure because no mathematical theorem forbids an eavesdropper (Eve) from building a clever algorithm, or a quantum computer, that will allow her to crack such codes.

On the other hand, private key cryptography can be unconditionally secure if encryption techniques such as the ‘one time pad’ are performed. The weakness of these techniques is that the key has to be securely transmitted by Alice to Bob. This can be done by using a courier, a plane ticket and a briefcase, but one then depends on the courier being honest.

Quantum cryptography elegantly solves this problem by enabling the unconditionally secure transmission of a random binary key between Alice and Bob, and hence is very often referenced as Quantum Key Distribution (QKD). Basically, the security of the transmission is ensured by the no-cloning theorem that forbids the perfect reproduction, or cloning, of a quantum system without disturbing it, therefore enabling Alice and Bob to detect the presence of a potential eavesdropper.



Now QKD networks are being formed in several places in the world. The QUAPITAL project (www.quapital.eu) aims at establishing a network in central Europe, with Trieste as Italia partner.

Scope of the research is to analyze how to create a QKD link within the city of Trieste, followed by a link between Trieste and Udine. Next, a link between Trieste and Ljubljana should be formed. The state of the fiber optics infrastructure should be analyzed, as well as the best strategy for sending entangled photons. First experiments should be performed.

Reference person: Angelo Bassi (abassi@units.it)

(Photo credit: IQOQI Vienna)