Contribution ID: **55**

Type: **not specified**

Cryptanalysis for trusted nodes in quantum key distribution

Friday, 29 January 2021 10:00 (10 minutes)

One of the major challenges of **quantum key distribution (QKD)** is the limited distance at which the communicating parties (Alice and Bob) can be. To mitigate this effect, **trusted nodes** are established, where the key is reconstructed and resent to more distant locations. But even though these nodes are trusted, they are still open to certain types of attacks, namely to the so-called "**side-channel attacks**", which can be exploited by quantum hackers.
The goal of this thesis is to calculate the limit of information which can be disclosed to an eavesdropper (Eve) in these trusted nodes while maintaining the key renewal perfectly secure. Moreover, we shall determine the impact of the number of trusted nodes on the key generation rate, assuming an upper limit of information disclosed by each node. We will also consider concrete QKD implementations at Instituto de Telecomunicações, based on optical fiber and on free space.

Primary author: BRAVO, João (Instituto Superior Técnico, ULisboa)

Presenter: BRAVO, João (Instituto Superior Técnico, ULisboa)