Contribution ID: **48** Type: **not specified**

26-Semi-Device Independent protocols for QKD

Wednesday 16 February 2022 15:44 (13 minutes)

The development of Quantum Computers poses a serious risk towards modern day encryption. To solve this problem, Quantum Key Distribution (QKD), a collection of protocols that use quantum mechanics to achieve encryption, was proposed. In these types of protocols quantum correlations are exploited to achieve QKD even with untrusted devices, a remarkable achievement. Any potential faults introduced intentionally or unintentionally are detected automatically making these protocols inherently more robust. There are a few drawbacks to DI cryptography, namely it's extreme difficulty of implementation in the lab. Therefore, it is more important to take realistic approaches when creating cryptographic protocols whilst trying to preserve the interesting ideas of device independence. Such protocols are known as Semi-Device independent (SDI) protocols and require a well-founded assumption about the measuring devices. These protocols are the subject of study in my master thesis where I will be looking at quantum correlations established between Alice and Bob with an energy bound on some quantum resource shared between them.

Author: JESUS, José (Instituto Superior Tecnico)

Presenter: JESUS, José (Instituto Superior Tecnico)