ICFO

ALUMNI SEMINAR: Semi-device-independent quantum key distribution with imperfect contextuality

VICTORIA WRIGHT

May 10, 2024
12:00 to 13:00
Blue Lecture Room

I will present a work in-preparation in which we derive semi-device-independent security proofs for prepare-and-measure QKD protocols. Witnessing a contextual correlation can provide a semi-device-independent certification of entropy between the trusted parties and any eavesdropper in a prepare-and-measure protocol. However, witnessing preparation-contextual correlations in an experiment requires one to assume that some preparation equivalence (such as basis independence) is exactly satisfied. Since it is impossible to prepare an exact quantum state, this requirement presents a problem. We navigate this problem by demonstrating that there always exists a set of hypothetical extra states that would augment a collection of imperfectly prepared quantum states such that they satisfy an exact equivalence. Under the connection between generalised contextuality and Bell non-locality, these extra states correspond to a no-click outcome for each of one party's measurements in the relevant Bell scenario. This hypothetical no-click would occur with probability bounded by the closeness of the imperfectly prepared states to their targets in the prepare-and-measure experiment. Using known entropy bounds from Bell inequality violations, we can then derive key rates for our protocol secure against collective attacks using observed statistics. We are studying under which assumptions these bounds can be combined with the generalised entropy accumulation theorem to give security against coherent attacks.

Hosted by: Prof. Dr. Antonio Acin