Contribution ID: **47** Type: **Talk**

Security of discrete-modulated continuous-variable quantum key distribution

Monday, May 29, 2023 3:10 PM (20 minutes)

Continuous variable quantum key distribution with discrete modulation has the potential to provide unconditional security using widely available optical elements and existing telecom infrastructure, while allowing for the use of well studied error correction protocols. However, proving finite-size security against coherent attacks poses a challenge. In this work we apply the entropy accumulation theorem, a tool that has previously been used in the setting of discrete variables, to prove finite-size security against coherent attacks for a discretely modulated QKD protocol involving four coherent states and heterodyne detection, under a realistic photon number cutoff assumption. Our analysis provides non-trivial key rates for $n = 10^{12}$ rounds.

Primary authors: Dr BAEUML, Stefan (ICFO); Mr PASCUAL, Carlos (ICFO); Dr WRIGHT, Victoria (ICFO); Prof. FAWZI, Omar (ENS Lyon); Prof. ACIN, Antio (ICFO)

Presenter: Mr PASCUAL, Carlos (ICFO)

Session Classification: Session 4.3