

Finite-key analysis in satellite quantum key distribution for 1-decoy and 2-decoy protocols

Tuesday, 14 February 2023 16:00 (2 hours)

The decoy state technique in quantum key distribution (QKD) has been proven as the most optimal strategy to counter photon number splitting (PNS) attacks. In the asymptotic limit of running the experiment an infinite time, it was shown that 2-decoy outperforms 1-decoy protocol. However, it was also showed that 1-decoy reached higher key rates than 2-decoy for finite block sizes except for short (below 79 km) and long (above 290km) distances. This analysis was performed for a simple channel loss. Here, we present a comparison for a free space channel. Our numerical simulation toolkit (SatQuMa) was used to compare the two decoy methods in a satellite scenario. Our research may provide implications in future satellite QKD missions.

Primary author: Mr POUSA, Roberto (University of Strathclyde)

Presenter: Mr POUSA, Roberto (University of Strathclyde)

Session Classification: Poster Session