Contribution ID: **30** Type: **not specified**

Realistic Thread Models for Satellite-based Quantum Key Distribution

Wednesday, 15 February 2023 12:10 (35 minutes)

We study the security of prepare-and-measure satellite-based quantum key distribution (QKD) in restricted eavesdropping scenarios where Eve has limited access to the transmitted signal by Alice. An artefact of such an assumption is the possibility of having bypass channels, those which are not accessible to Eve, but may not necessarily be characterized by the users either. This creates interesting scenarios for analyzing QKD security. Here, we present generic bounds on the key rate in the presence of bypass channels and apply them to continuous-variable QKD protocols with Gaussian encoding with direct and reverse reconciliation. We find regimes of operation in which the above restrictions on Eve can considerably improve system performance. We also develop customised bounds for several protocols in the BB84 family and show that, in certain regimes, even the simple protocol of BB84 with weak coherent pulses is able to offer positive key rates at high channel losses, which would otherwise be impossible under an unrestricted Eve. Our work opens up new security frameworks for spaceborne quantum communications systems.

Primary author: RAZAVI, Moshen (University of Leeds)

Presenter: RAZAVI, Moshen (University of Leeds)

Session Classification: Space QKD