Contribution ID: **37** Type: **Poster**

Security of Decoy-State Quantum Key Distribution Against Trojan-Horse Attacks

Most security proofs of quantum key distribution (QKD) disregard the effect of information leakage from the users'devices, and, thus, do not protect against Trojan-horse attacks (THAs). In a THA, the eavesdropper injects strong light into the QKD apparatuses, and then analyzes the back-reflected light to learn information about their internal setting choices. Only a few recent works consider this security threat, but predict a rather poor performance of QKD unless the devices are strongly isolated from the channel.

We present an improved finite-key security analysis for decoy-state-based QKD schemes in the presence of THAs, which significantly outperform previous analyses. For this, we take advantage of the reference technique [Science Advances, 6(37), eaaz4487] equipped with a Cauchy-Schwarz-based constraint to incorporate the information leakage from the bit/basis and intensity encoding setups in the security analysis. This requires the users to bound a single parameter that encapsulates all the imperfections, which in practice can be directly related to the amount of isolation of Alice's transmitter. Besides, we use novel concentration bounds to deal with the finite-key effects.

For illustration purposes, we evaluate the performance of the standard decoy-state BB84 protocol and the decoy-state loss-tolerant protocol in the presence of THAs. The results demonstrate the feasibility of both schemes over long distances given that the information leakage is small enough, which could be achieved by increasing the isolation of the devices. Besides, for the decoy-state BB84 case, we compare the secret-key rate attainable with our security proof with that obtained in previous analyses [New Journal of Physics, 20(8), 083027]. The results show that our analysis basically allows to double the maximum achievable distance attained by previous works in some realistic scenarios.

Author: NAVARRETE RODRIGUEZ, Álvaro (Universidad de Vigo)

Co-author: Prof. CURTY, Marcos (Universidad de Vigo)

Presenter: NAVARRETE RODRIGUEZ, Álvaro (Universidad de Vigo)

Session Classification: Poster Session 1