Real Sociedad Española de Física

ID de la contribución : **280** Tipo : **Oral parallel contribution**

Measurement-Device-Independent Quantum Key Distribution with Information Leakage

martes, 18 de julio de 2017 18:05 (20)

Measurement-device-independent quantum key distribution (MDI-QKD) is proposed to remove all the detection side-channels in quantum communication systems. In recent years, MDI-QKD has been proven to be secure with certain assumptions and become a significant step toward the practicality of QKD systems. However, the assumption that there is no information leakage from the security zones of the legitimate parties seems very difficult to be guaranteed in practice. In this work we relax this assumption by proposing a general formalism to prove the security of MDI-QKD in the presence of information leakage. Particularly, we analyze a specific Trojan-Horse attack on the intensity modulator and phase modulator and the secure key rates under different amounts of information leakage are calculated in several practical cases. Our work provides an essential reference for experimentalists to ensure the security when implementing MDI-QKD protocols in the presence of information leakage.

Primary author(s) : Sr. WANG, Weilong (University of Vigo)

Co-author(s) : Sr. CURTY, Marcos (University of Vigo)

Presenter(s) : Sr. WANG, Weilong (University of Vigo)

Clasificación de la sesión : Quantum Technologies: joint symposium of the Quantum Information and Quantum and Non-linear Optics specialised groups

Clasificación de temáticas : Quantum Information