World Academy of Science, Engineering and Technology
International Journal of Nuclear and Quantum Engineering
Vol:13, No:03, 2019

Proposal of Optimality Evaluation for Quantum Secure Communication Protocols by Taking the Average of the Main Protocol Parameters: Efficiency, Security and Practicality

Authors : Georgi Bebrov, Rozalina Dimova

Abstract : In the field of quantum secure communication, there is no evaluation that characterizes quantum secure communication (QSC) protocols in a complete, general manner. The current paper addresses the problem concerning the lack of such an evaluation for QSC protocols by introducing an optimality evaluation, which is expressed as the average over the three main parameters of QSC protocols: efficiency, security, and practicality. For the efficiency evaluation, the common expression of this parameter is used, which incorporates all the classical and quantum resources (bits and qubits) utilized for transferring a certain amount of information (bits) in a secure manner. By using criteria approach whether or not certain criteria are met, an expression for the practicality evaluation is presented, which accounts for the complexity of the QSC practical realization. Based on the error rates that the common quantum attacks (Measurement and resend, Intercept and resend, probe attack, and entanglement swapping attack) induce, the security evaluation for a QSC protocol is proposed as the minimum function taken over the error rates of the mentioned quantum attacks. For the sake of clarity, an example is presented in order to show how the optimality is calculated.

Keywords : quantum cryptography, quantum secure communcation, quantum secure direct communcation security, quantum secure direct communcation efficiency, quantum secure direct communcation practicality
Conference Title : ICQOQC 2019 : International Conference on Quantum Optics and Quantum Computing
Conference Location : London, United Kingdom
Conference Dates : March 14-15, 2019