Ph.D. Thesis

Name of the Candidate: Rajni Bala

Entry Number: 2016PHZ8379

Title of the Thesis: Error-immune and secure quantum communication with optimal resources

Abstract

In recent times, quantum communication has emerged as a vibrant area of research. The horizon of quantum communication has numerous celebrated and pioneering protocols— quantum teleportation, quantum key distribution, error-correction-assisted quantum communication protocols. Challenges and limitations in the generation of resources required for these protocols nevertheless act as major impediments. An indispensable problem is in making experimental realizations and theoretical assumptions come hand in hand. Elegant protocols like quantum teleportation and Ekert 91 QKD employ entangled states, whose generation poses a challenge. In particular, error correction poses a significant challenge in quantum communication since the application of higher dimensional entangling gates in many degrees of freedom, e.g., OAM is not readily available. This leads us to the question of interest in this thesis: to what extent can we alleviate the need for costly quantum resources and still have a quantum advantage, albeit in some restricted scenarios? We attempt to answer this question in the context of error-immune quantum communication and quantum key distribution — two cornerstones in the area of quantum communication.

In the first part of the thesis, we focus on laying down a resource-friendly approach to error-immune quantum communication. In contrast to the traditional approaches, which encode information in a quantum state, we develop a framework by proposing an altogether new information encoding scheme. This scheme, by construction, encodes information in the invariants of a noisy channel. Notably, this encoding scheme leads to a complete removal of budget overhead for quantum error correction. We construct invariants for several noisy channels which are of practical interest. Interestingly, quantum error-correcting and rejecting codes appear as special cases of this encoding scheme. Finally, we have applied the framework to a practical situation of propagation of OAM modes in turbulence. By performing a study of extensive simulation data, we phenomenologically model the channel as an idealized crosstalk channel and identify the invariants for the same. These invariants serve the purpose of being error-immune information carriers.

In the second part of thesis, we turn our attention exclusively on resource-friendly quantum key distribution protocols. In this direction, a significant development is the proposal of semi-quantum key distribution protocol. This protocol involves only one quantum participant who can operate in any basis, in contrast to a classical participant who can operate only in the computational basis.
We perform a series of studies to propose quantum and semi-quantum key distribution protocols by employment of OAM states of light, which are arguably at the forefront of realization of high dimensional quantum communication. We start by showing that the task of secure distribution of keys in layered networks can be accomplished with only one quantum participant and multidimensional separable states. We believe that this is a significant development over the protocols proposed in [Pivoluska et al. Physical Review A 97.3 (2018): 032312], which employ multidimensional entangled states with a very low generation yield. In the second study, we show that corresponding to every nonlocality/entanglement-based QKD protocol, a contextuality-based QKD protocol may be designed. The security analysis of the latter protocol is, however, completely different and hinges on masking transformations. The key rate of the CQKD protocols, however, is exponentially small. As the next improvement, we show how a suitable change in the key generation rule and the choice of observables may lead to enhancement in the key generation rates with the same resource states. Finally, we show that qubits encoded in qudits may be employed for QKD protocols. The generation yield of these states is significantly high. We have shown robustness of all the protocols to eavesdropping attacks.