Enhanced tight finite key scheme for quantum key distribution (QKD) protocol to authenticate multi-party system in cloud infrastructure

ABSTRACT

This research is introducing an enhanced tight finite key scheme for quantum key distribution (QKD) protocol to authenticate multi-party system in cloud infrastructure. The main attraction is to provide a secure channel between a cloud client to establish a connection among them by applying the theories from Von Neumann and Shannon entropies and also Shor's algorithm. By generalizing these theories we will produce enhanced tight finite key scheme for quantum key distribution (QKD) protocol to authenticate multi-party system in cloud infrastructure. Hence we are using quantum channel and also quantum key distribution (QKD) together with BB84 protocol replacing common channel to distribute the key. We are proposing an authentication of multi-party Quantum Key Distribution (MQKD) protocol using an enhanced tight finite key scheme because it will involve a number of parties in cloud infrastructure. Significant of this research is to reduce the possibility of losing a private key by producing a high efficient key rate and attack resilient.

Keyword: Authentication scheme; Cloud infrastructure; Multi party; Quantum key distribution