Different useful aspects of hierarchical quantum communication

Abstract

Many schemes of multi-party quantum teleportation (symmetric quantum information splitting) have been proposed in last two decades and that led to a set of interesting applications like the controlled teleportation (CT) or the quantum information splitting (QIS) schemes. There are many aspects of quantum communication like probabilistic QIS, quantum secret sharing (QSS) which may be viewed as an application of QIS. Recently, Wang et al. [1]-[3] introduced the concept of asymmetric quantum information splitting, which is known as hierarchical quantum information splitting (HQIS) scheme, using a 4-qubit Kai state [1]. Subsequently they extended their idea to t-qubit graph state with $t \geq 3$ [2], and a 6-qubit cluster state [3]. In HQIS there is a hierarchy in power to recover the quantum state sent by Alice among the agents. We have extended the idea of Wang et al. and have proposed a systematic and general procedure to investigate the possibility of HQIS using an arbitrary (n + 1)-qubit entangled state [4]. We have also shown that HQIS is possible for different classes of 4-qubit entangled quantum states. Our scheme is further modified to introduce protocols of probabilistic HQIS, and hierarchical quantum secret sharing (HQSS). The proposed schemes are interesting and important because of their relevance in many practical situations like banking, departmental stores, etc. Further the existence of HQIS automatically implies the existence of many related aspects of controlled teleportation (e.g. controlled quantum information splitting, controlled quantum secret sharing, controlled quantum state sharing etc.). The relevance of the protocols described here are elaborated with appropriate importance.

Key words: Hierarchical quantum information splitting (HQIS), Hierarchical quantum secret sharing (HQSS), quantum communication.

Some practical situations where we can use HQIS and HQSS:

In realistic situations of our practical needs in daily life, hierarchy in secret sharing is everywhere in the classical world like banking, big bazaar, departmental stores, universities companies and many more places.

1) Suppose, Alice is boss of a company and Bob, Charlie and Diana are her agents. Alice trusts Diana more than the other two agents as he is the oldest employ. Thus there is a hierarchy among the agents. In this situation, Alice may use HQIS scheme with 4-qubit Omega states as described in case-I [4] and send the information in three pieces so that none of Bob, Charlie and Diana can read the message of Alice without the help of the other.

2) Another sector where HQSS is of everyday need is banking: In bank lockers you can open it with two keys, one key remains with bank and other with the user, only when both are used then the locker opens but these classical keys are not unconditionally secure, so in this situation, HQSS can give us an unconditionally secure bank-vault. Why hierarchy: Assume that Bob is manger and Charlie is user and Diana is regional manager (some big boss of the bank), if Diana permits then Charlie and Bob goes to the vault, uses there keys and open the locker but user (Charlie) is a criminal and kept some murder weapon in the locker, now CBI wants to see what is inside the locker now Diana can take help of manager (Bob) and show the locker to CBI, they do not need the help of Charlie, this is how exactly things work in bank locker.

3) In a bank a bank manager and/or cashier is usually more powerful than the other users (office assistants and secretaries). However, even the bank manager alone is not powerful enough to perform all the financial operations related to his bank. For example, the password required to unlock an ATM is always split into two or more pieces and the manager alone cannot unlock it. Similarly, hierarchical secret sharing is also essential for the smooth operation of the departmental stores.

References

[1] X.-W. Wang, L.-X. Xiac, Z.-Y. Wangd, D.-Y. Zhang, Opt. Comm. 283 (2010) 1196.

[2] X.-W. Wang, D.-Y. Zhang, S.-Q. Tang and L.-J. Xie, J. Phys. B 44 (2011) 035505.

[3] X.-W. Wang, D.-Y. Zhang, S.-Q. Tang, X.-G. Zhan, K.-M.You, Int. J. Theor. Phys. 49 (2010) 2691.

[4] C. Shukla and A. Pathak, arXiv: 1301.0498v1 [quant-ph].