A class of Variable Multi-party Quantum Key Protocols based on Repetitive code

Li Lei, Xidian University, China. （leil.lilly@qq.com）

Abstract With the maturity of the two-party quantum key distribution technology, people began to pay attention to the expansion of the quantum key distribution protocol, that is, to study the multi-party quantum key distribution protocol (MQKD). However, as the number of participants increases, this type of protocol is facing two main issues, one is the efficiency of the agreement, the other is to ensure the security of information. In terms of ensuring information security, there are three elements: in order to ensure that the information is not eavesdropped by others, transmission encryption can be carried out; in order to ensure that the identity of participants cannot be stolen by others, encryption algorithms can be used for identity demonstration; in order to ensure that the transmission content is not tampered, an encryption algorithm can also be used for digital authentication. In the multi-party quantum key related agreement, these three elements must be ensured. Most of these protocols can encrypt information during transmission or prevent eavesdropping, but it is difficult to meet the latter two at the same time. However, in real life, there may be dishonest participants. Therefore, in order to obtain a truly secure key, it is necessary to verify the authenticity of the participant's identity and the obtained quantum key.

How to design a multi-party quantum key distribution protocol that can ensure information security, and can further improve its efficiency and quantum resource consumption, is a very worthy study. In this article, we will focus on QKD based on unbiased basis, and design a new verifiable multi-party QKD protocol using repeated codes for the first time. The protocol is composed of two parts: the classical network and the quantum network. The classical network adopts the Shamir (t, n) threshold scheme that based on a binary polynomial. The secrets recovered by the participants of the classical network and the session keys they obtain are used in the relevant parameters of the quantum network protocol to ensure the security of the information, and the designed quantum key distribution protocol can verify the identity of participants.

Contributions of this agreement are as follows:

1. High efficiency. It is the first time to use the repetitive code theory to encode quantum information sequences, so that the protocol can prevent eavesdropping without deceiving state particles. Therefore, the protocol is highly efficient and saves quantum resources.
2. Identity authentication function. Using the relevant data in the bivariate polynomial theory as the relevant parameters in the quantum key distribution protocol ensures the identity authentication between participants.
3. The function of verifying information. Use the private key s generated in the shamir threshold scheme as the key of the hash function to verify the accuracy of the information in the quantum key distribution protocol.
4. Scalability. In the quantum system model, we assume that each terminal has the function of generating, manipulating, and measuring single photons. Under such conditions, our protocol is suitable for multi-party participants to transfer quantum keys.

Finally, we compared our agreement with several current multi-party QKA agreements. Due to the use of the technology of repeated codes and the classic binary polynomial theory, our scheme has significantly improved efficiency, less complexity, and ensures the security of information and the identity authentication function between participants.