Quantum homomorphic signature

Tao Shang, Xiao-jie Zhao, Chao Wang, Jian-wei Liu
School of Electronic and Information Engineering, Beihang University, Beijing 100083, China

Quantum signature which concerns about the authenticity and non-repudiation of messages on insecure quantum channels is an important research topic in quantum cryptography. So far, a few quantum signature schemes have been proposed. Inspired by entanglement swapping, we first propose a new quantum homomorphic signature scheme which can be used to authenticate data packets of multiple streams for quantum networks. After combining two quantum signatures by entanglement swapping, it can generate a new homomorphic signature at the intermediate node. The proposed homomorphic quantum signature scheme can effectively guarantee the security of secret key and verify the identity of different data sources in a quantum network.

In order to authenticate the identity of data source in a network, homomorphic signature scheme is considerably paid attention to instead of standard signature schemes in classical cryptography. However, homomorphic signature schemes of classical information are inapplicable in quantum networks. It is believed that homomorphic signature of quantum information is more meaningful and difficult than its counterpart in classical cryptography. Particularly, homomorphic signature in form of quantum states is desired for quantum networks. On one hand, the main problem is how to design a signature operation for quantum states. On the other hand, the authentication of different data sources is also a very hard problem for classical networks, so it is necessary to explore whether it is a hard problem for quantum networks or not. If quantum homomorphic signature scheme is feasible, it will be very helpful to enhance the security of quantum networks. However, a solution to quantum homomorphic signature still remains open. It is crucial to find an equivalent quantum homomorphic operation to realize signature computing in form of quantum states. Until now, there is no obvious way to combine two quantum signatures from the senders to realize a homomorphic operation due to the properties of quantum mechanics.

A general quantum signature model is conjectured just as shown in Figure 1. By sharing an EPR pair (denoted as $|\psi\rangle_{12}$) with a verifier *V*, a signer *A* can sign on its classical information *X* by means of performing a corresponding unitary operation on its particle 2. For the aggregation of multiple signatures, it is the most straight idea to guarantee that each signer shares an EPR pair with the aggregator *C*, then the aggregator generates a new signature. Just as described in Figure 1, the key is to generate a new homomorphic signature $S_3 = U(X_1 \oplus X_2)\cdot|\psi\rangle_4$ at the aggregator *C* according to two signatures S_1 and S_2. As far as we know, no quantum signature schemes have been proposed to combine homomorphic algorithm till now. The existing quantum signature schemes are also not suitable for quantum network just as described in Introduction. Hence it is significant to investigate the design of quantum homomorphic signature for the authentication of data sources in quantum networks.

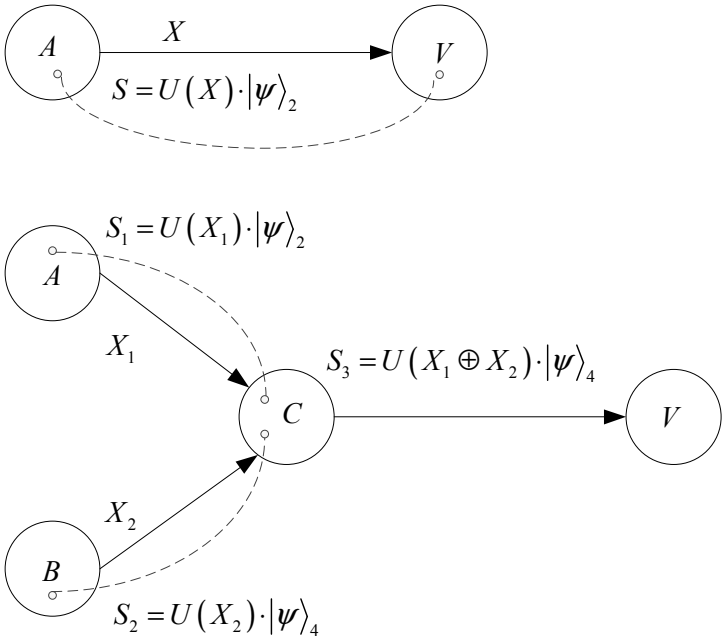

Fig. 1. Quantum signature model

Entanglement swapping is a miracle property of quantum entanglement. The key idea of entanglement swapping is that two non-entangled particles (1, 3) become an entangled state by measurement. Note that if we treat the particles 2 and 4 as two signatures, we can transform these two signatures into an entangled state without original data by means of entanglement swapping. Then in the new entangled state, the particle 4 can be treated as a new signature. This result gives an important hint of relationship between entanglement swapping and homomorphic operation. The key to the design of homomorphic operation is to make the particle 4 become the homomorphic signature result of combining two original signatures. Hence entanglement swapping provides the possibility of homomorphic operation for quantum signature. Concretely, the main contributions of our work are: (1) A homomorphic operation for quantum states is first found. The homomorphic operation is the key part of quantum homomorphic signature. We delicately utilize entanglement swapping for the homomorphic operation which satisfies homomorphic property for the operation of quantum states. (2) Quantum homomorphic signature scheme is first proposed. The property of quantum homomorphic signature scheme is derived. It contributes to the signature operation in the bottleneck nodes of quantum network. It also contributes to the authentication of multi-source unicast stream or single-source multicast stream. Our scheme provides a convenient model to combine authentication into quantum networks, which would be significant to enhance the security of quantum communication.

According to the above approach, our scheme can be easily extended to multi-source model which may contain *n* source nodes. Moreover, it can solve the problem of identity authentication of single-source unicast, single-source multicast, multi-source unicast, or multi-source multicast in quantum networks. Hence homomorphic signature scheme can generate a new signature on its message without the private keys of data sources, which is very important to distributed networks and can be used to generate new signatures at intermediate nodes through directly manipulating the original signatures of received messages without encryption operation.