Can we have a secure Quantum network?

Zheng-Hong Li,[1] M. Al-Amri,[2,3] Xihua Yang,[1] and M. Suhail Zubairy[3]

[1] *Department of Physics, Shanghai University, Shanghai 200444, China*
[2] *The National Center for Applied Physics, KACST, P.O.Box 6086, Riyadh 11442, Saudi Arabia*
[3] *Institute for Quantum Science and Engineering (IQSE) and Department of Physics and Astronomy, Texas A&M University, College Station, Texas 77843-4242*

(Dated: April 25, 2017)

An arbitrary unknown quantum state can not be cloned. The statement which is known as quantum no-cloning theorem later indicates a robust way to secure communication. Based on that, the first quantum key distribution protocol (QKD), BB84, is published in 1984, which allows two communicators to generate a unique random key. This is a milestone of quantum cryptography. Clearly, there has been intense of research during the past three decades on secure quantum communication resulting on having many published protocols. These are not only QKD protocols, but also include direct secure quantum communication protocols, quantum public-key cryptography and other more practical application techniques such as decoy states, device independent QKD. In addition, aimed at practical Recently, lots of efforts have been put to build a practical secure quantum network.

No doubt, quantum secure network has a bright future, while QKD is the most pretrial one for application. For security reasons, the distributed key in QKD is normally disposable, which is called one time pad. However, this brings a problem when more than two communicators are involved, i.e., the key management problem[1]. Since all keys are used once and discarded, they are meaningless to be shared among all communicators. Needless to say that when the number of communicator increases, there are will be a huge number of keys to be in place and more importantly wisely managed. This takes lots of resource.

Then, a question of interest is: Can we create and share a key among more than two users? Some good results have been published such as quantum public-key cryptography [1, 2], which utilizes quantum one-way function. Here, there are two keys; a public key to encode message, while a private one for decoding message. Hence, a receiver manage to collect information from a large number of senders since he holds the private key.

In this paper, however, we solve the key management problem from a different angle. We propose a secure direct quantum communication protocol that allows secure messages to be shared among multiple authorized users. Our protocol is based on Ping-Pong protocol. By phase control in one arm of a Mach-Zehnder interferometer, information is transferred directly and certainly due to path entanglement. Apparently, many interferometers can be controlled simultaneously so that one can broadcast his messages to many receivers. Security is a big issue and a protocol like Ping-Pong, security is generated by random check utilizing entanglement between photon paths. However, a recent work [3] indicates that current security strategy is no longer safe, particularly, when an almost "invisible" photon can reveal the single-photon detector without alerting it. Furthermore, [4] shows that the phase operation acted on the photon also can be found out by the "invisible" photon. This can be used as an attack, and we call it counterfactual attack. Hence, it is highly important to defeat this attack, here, we propose a multi-users authorization system that work based on sharing a secure message/key among multi-users. This way, a quantum secure group communication protocol is achieved. Emphasizing that the main principle of protection is based on path entanglement and it is impossible for Eve to find out which path information without disturbing the interference.

[1] G. M. Nikolopoulos, Phys. Rev. A **77** 032348 (2008).

[2] E. Andersson, M. Curty, and I. Jex, Phys. Rev. A **74** 022304 (2006).

[3] H. Salih, Z.-H. Li, M. Al-Amri and M. S. Zubairy, Phys. Rev. Lett. **110** 170502 (2013).

[4] Z.-H. Li, M. Al-Amri and M. S. Zubairy, Phys. Rev. A. **89** 052334 (2014).