Physics Letters A 380 (2016) 2349–2353

Contents lists available at ScienceDirect

Physics Letters A

www.elsevier.com/locate/pla

Multi-group dynamic quantum secret sharing with single photons

Hongwei Liu [a], Haiqiang Ma [a,*], Kejin Wei [a], Xiuqing Yang [b], Wenxiu Qu [a], Tianqi Dou [a], Yitian Chen [a], Ruixue Li [a], Wu Zhu [a]

[a] School of Science and State Key Laboratory of Information Photonics and Optical Communications, Beijing University of Posts and Telecommunications, Beijing 100876, China
[b] School of Science, Beijing Jiaotong University, Beijing 100044, China

ARTICLE INFO

Article history:
Received 6 December 2015
Received in revised form 18 May 2016
Accepted 19 May 2016
Available online 24 May 2016
Communicated by P.R. Holland

Keywords:
Quantum cryptography
Quantum information
Quantum secret sharing

ABSTRACT

In this letter, we propose a novel scheme for the realization of single-photon dynamic quantum secret sharing between a boss and three dynamic agent groups. In our system, the boss can not only choose one of these three groups to share the secret with, but also can share two sets of independent keys with two groups without redistribution. Furthermore, the security of communication is enhanced by using a control mode. Compared with previous schemes, our scheme is more flexible and will contribute to a practical application.

1. Introduction

In recent years, information disclosure occurs constantly, which has made people aware of the importance of protecting sensitive data. However, classical cryptography, based on computation, has encountered an unprecedented threat from breakthroughs in quantum computation. Fortunately, the presentation of the first quantum key distribution (QKD) protocol by Bennett and Brassard in 1984 [1], known as protocol, broke new ground for achieving the Holy Grail of cryptography-unconditional security in communication. Since then, researchers have proposed many QKD systems [2–7].

The common feature among these systems is that a secret key is owned by only one agent, which cannot meet the requirements of some high security missions. A missile launch, for example, is protected by a secret key, but, a single administrator must not be able to activate it alone. Conventional cryptography provides a solution known as secret sharing [8], but it is susceptible to eavesdropping attacks because of the mathematical algorithms used. In 1999, a protocol [9], proposed by Hillery et al., introduced quantum cryptography to secret sharing. This protocol is referred to as quantum secret sharing (QSS). Thus far, many theoretical and experimental QSS schemes [10–14] have been proposed. However, a situation which occurs frequently in practical applications, but has not been considered thus far, concerns the volatility of the agents. Recently, dynamic QSS protocols [15,16] based on entangled states have been proposed to solve the above-mentioned problems. The so-called hierarchical QSS protocol has also been proposed [17], aimed at improving the freedom of QSS and its freedom focused on the unequal power of agents to reconstruct the Boss' secret, namely, that high-grade agents need less help from others. In practical situations a realistic scheme of secret sharing should have both features. Fortunately, a hierarchical dynamic QSS protocol [18] has been proposed recently and the possibility that any existing protocol of quantum communication can be implemented has been discussed.

Here, we provide a novel solution scheme based on single photons to enhance the freedom of QSS, in which the groups added or dropped are considered. In our scheme there are three groups, one of which includes one boss, Alice, and three groups of agents. The first and second groups are Bob_i and Charlie_i respectively, where $i \in \{1, 2\}$ denotes the number of group; all the agents together comprise group three. Alice can dynamically select any one of the groups to complete secret sharing through controlling the polarization states of launched photons. Furthermore, two independent secret keys can be shared to groups one and two simultaneously. Although the dynamic degree in our current work is lower than that of the protocols proposed in [15,16], which use cluster states [15] and entanglement swapping [16] to fulfill the complete dynamic, including an agent joining or leaving the QSS, our multi-group dynamic QSS with single photons scheme, whose dynamic lies in the feature that a group can always be added or dropped, will contribute to furthering development. This has direct practical relevance in real life situations. Consider a government or a

* Corresponding author.
E-mail address: hqma@bupt.edu.cn (H. Ma).

http://dx.doi.org/10.1016/j.physleta.2016.05.032
0375-9601/

company which has various departments and of which Alice is a president. Now, depending on the different assignments, she may want to add or drop a department in a built quantum network. Our current work allows this dynamic among groups, as long as the agents in one group have an equal grade. We also propose an experimental implementation, which is scalable since the additional parties can be connected to the arm of a beam splitter (BS) with a three-port or four-port PBS (FPBS) linking a Faraday mirror (FM). In principle, when more parties are added, the total loss of the system will increase, but the visibility of the system will basically remain unchanged [13]. This design is important to our scheme, because it can provide completely polarization-insensitive phase modulation, which means any polarized pulse can be modulated by agents in our system [13,14]. Furthermore, the stability of the system is ensured by using a FM terminating a single-mode fiber (SMF), which can auto-compensate for the birefringence of the fiber [19,20]. These components are widely used in commercial QKD systems [2,21].

2. Protocol

Before proceeding to our scheme, it is beneficial to introduce the workflow of the Deng's protocol [11]. The boss, Alice, uses two sets of conjugate measuring bases to randomly prepare her qubits $|j\rangle$ into one of the following four states:

$$|j\rangle \in \{|+z\rangle, |-z\rangle, |+x\rangle, |-x\rangle\} \tag{1}$$

where

$$|+z\rangle = |0\rangle, |-z\rangle = |1\rangle, \tag{2}$$

$$|+x\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), |-x\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle). \tag{3}$$

Bob and Charlie choose the coding mode, and randomly perform one of the two unitary operations, U_0 and U_1, on the single photons received.

$$U_0 = |0\rangle\langle 0| + |1\rangle\langle 1|, \tag{4}$$

$$U_1 = |0\rangle\langle 1| - |1\rangle\langle 0|. \tag{5}$$

Fig. 1 shows the process of this protocol. For the sake of the protocol security, all parties must add a small trick in this process. For each photon received, Bob and Charlie need choose the control mode or the coding mode randomly for each photon. In the control mode, the photon is measured by one of the two measuring bases randomly. Alice performs the measurement on most of the received photons with the same base as she used to prepare her qubits. As the two unitary operations, U_0 and U_1, do not change the measuring bases, Alice obtains a deterministic outcome for almost all the photons returned, e.g. $U_A = U_B \otimes U_C$, where U_B and U_C are the operations performed on the same photon by two agents respectively, and U_A is the total operation on the photon. For others, she performs the same operation as Bob and Charlie did in the control mode. After analyzing the error rates by comparing the results of the measurement that they publish and confirming a security quantum communication, a raw key for distilling is shared. This key will be known by agents if and only if they cooperate with each other. The security of this protocol has been proved in a similar way to those used in [1,22,23].

In our scheme, all the agents are divided into n groups. Alice first prepares a single photon in the qubit state $|\psi_A\rangle$, chosen uniformly at random from the following set:

$$|\psi_A\rangle \in |P_i\rangle \otimes |j\rangle, \tag{6}$$

where $|P_i\rangle$ indicates that this is a qubit in the polarization degree of freedom (DOF) of the photon, and i is the group with which

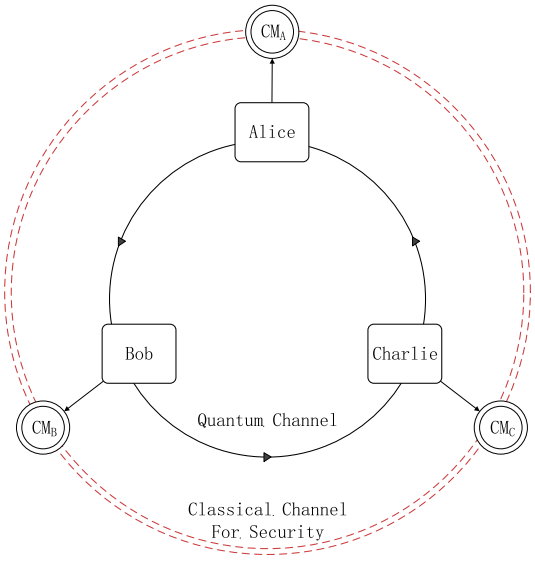

Fig. 1. Protocol of circular quantum secret sharing. CM denotes control mode. Alice, Bob and Charlie randomly choose the control mode for security. The full line represents the quantum channel and the double dashed line is the classical channel.

Alice wants to share. If these photons are prepared in the superposition state

$$|\psi_A\rangle \in \sum_{i=1}^{m} |P_i\rangle \otimes |j\rangle, m \leq n \tag{7}$$

Alice will simultaneously share the secret key with $m+1$ groups. Group $m+1$ is all the agents in all m groups. Their key is $k_{m+1} = \bigoplus_{i=1}^{m} k_i$, where $\oplus$ denotes modulo two addition.

The superposition state $|\psi_A\rangle$ is then sent to corresponding agents, randomly operated on by $|P_i\rangle\langle P_i| \otimes U_0$ or $|P_i\rangle\langle P_i| \otimes U_1$, and returned back to Alice. Alice performs the measurement on the received photons with the same base that she used to prepare her qubits. In order to identify to which group the photon has collapsed after measurement, the time-bin DOF of the photon must be added and analyzed. In the end, Alice broadcasts the groups she has chosen to share her secret with through the public channel, and the agents in these groups will know the secret key if and only if they work together.

3. Implementation

The setup of the proposed scheme, shown in Fig. 2(a), can be divided into two main parts: Alice's station and other parties' stations (Bob$_i$'s and Charlie$_i$'s, where $i \in \{1, 2\}$).

A laser pulse, whose polarization is controlled by a polarization controller (PC), is split into two pulses, P_1 and P_2, by BS_1. Pulse P_1, transmitting along the long arm L_a, is randomly modulated by a phase modulator (PM_A) to have a phase $\phi_A \in \left\{0, \frac{\pi}{2}, \frac{3\pi}{2}, \pi\right\}$ and reflected back to the BS_1 by FM_1, while pulse P_2 along the short arm S_a is directly reflected by FM_2 and comes back to BS_1. The pulses are coupled to a fiber and are attenuated to a pseudo single-photon level by an attenuator (ATT). Then these two pulses pass through a circulator (Cir_1) and an ordinary 50/50 beam splitter (BS_2) in sequence, and are divided into two clockwise pulses, P_{1U} and P_{2U}, and two counterclockwise pulses, P_{1D} and P_{2D}, due to the wave-like property of photons. Finally, these four pulses pass through two four-port polarization beam splitters, $FPBS_1$ and $FPBS_2$, arriving at Bob$_i$ and Charlie$_i$, where $i \in \{1, 2\}$ determined by the polarization Alice has chosen.