CONTROLLED QUANTUM KEY DISTRIBUTION WITH THREE-PHOTON POLARIZATION-ENTANGLED STATES VIA THE COLLECTIVE NOISE CHANNEL

Li Dong[a,b], *Xiao-Ming Xiu*[a,b*], *Ya-Jun Gao*[b], *Xue-Xi Yi*[a**]

[a] *School of Physics and Optoelectronic Technology, Dalian University of Technology*
Dalian 116024, P. R. China

[b] *Department of Physics, School of Mathematics and Physics, Bohai University*
Jinzhou 121013, P. R. China

Received January 27, 2011

Using three-photon polarization-entangled GHZ states or W states, we propose controlled quantum key distribution protocols for circumventing two main types of collective noise, collective dephasing noise, or collective rotation noise. Irrespective of the number of controllers, a three-photon state can generate a one-bit secret key. The storage technique of quantum states is dispensable for the controller and the receiver, and it therefore allows performing the process in a more convenient mode. If the photon cost in a security check is disregarded, then the efficiency theoretically approaches unity.

1. INTRODUCTION

The two recent decades have witnessed rapid development in the theory and practice of quantum communication. As a relatively mature technique, quantum key distribution (QKD) enables two legitimate users to establish a shared secret string of bits as a key for encrypting and decrypting secret information. In 1984, Bennett and Brassard put forward the pioneering four-state QKD protocol, BB84 [1], which is the first unconditionally secure key distribution protocol. Decreasing the practical complexity and halving the idealized maximum efficiency of BB84, Bennett presented a protocol with two nonorthogonal states in 1992, B92 [2]. Both these protocols are based on single-particle states. In 1991, Ekert proposed a QKD protocol based on Einstein–Podolsky–Rosen (EPR) pairs, E91 [3]. In 1992, by simplifying the complicated Bell inequality to two sets of nonorthogonal bases in the security check, Bennett et al. modified the E91 protocol to BBM92 [4]. Since then, QKD has attracted extensive attention of the researchers and progressed quickly [5–16].

Currently, photons are promising candidates for carriers of quantum information because they are cheap, fast, and interact weakly with the environment. But in actual applications, the polarization of photons is prone to be influenced by thermal and mechanical fluctuations and the imperfections of a quantum channel (e. g., the inhomogeneity of the atmosphere in free space, the birefringence in an optical fiber, misalignment of the reference frame, and backward emission [17]), which can be generally regarded as channel noise.

When the noise between the information carriers and the environment is sufficiently weak, the error arises with a low probability. Using a quantum error correction code, the participants utilize several physical bits as one logical bit according to the special noise, and then detect the stabilizer codes and correct them according to the detected result [18–20]. Entanglement purification [21–25] is also a method of error correction, which can achieve a subset of maximally entangled states from an entangled system after infinite operations.

There is a general assumption about the noise, the unitary collective noise model, in which the spatial (temporal) separation between the first and the last transmitted photons is smaller than the correlation length (time) of the environment. For instance, if the photons are nearly simultaneously transmitted or are

[*] E-mail: xiuxiaomingdl@126.com

[**] E-mail: yixx@dlut.edu.cn

sufficiently close to each other in space, the effect of the noise on each photon is identical, that is, the error of the physical channel is collective. We suppose that a unitary transformation $U(t)$ is an overall time-dependent action on a single photon, such that the whole effect of this kind of noise on the physical system can be represented as [26]

$$\rho_N \rightarrow [U(t)]^{\otimes N} \rho_N [U(t)^{\dagger}]^{\otimes N}, \qquad (1)$$

where t is the transmission time and N is the number of photons.

In order to cope with the collective noise, some noise models were constructed and many methods were studied to remove or decrease the noise. An active-feedback alignment system [27] can be adopted to conquer this kind of noise, in which the participants detect the noise consecutively and perform instant self-compensation according to the evaluated result of noise. But this method is difficult to realize because it interrupts the transmission process. Furthermore, if the performing compensation is slower than the variation of noise, the method does not work.

Based on the phase difference of single photons in two consecutive time bins, the phase-time coding QKD schemes under noise can be achieved with unbalanced interferometers (Mach–Zehnder interferometers) [2, 28], in which very demanding setups and conditions (e. g., complex interferometric setups, high precision timing, and stable low temperatures) are required to adjust the difference. Exploiting the Faraday orthoconjugation effect, the noise due to polarization fluctuations can be automatically and passively circumvented [29]. However, this requires two-way communication [30, 31], which makes the method vulnerable to a Trojan horse attack.

For solving the problem of bit-flip error, Bouwmeester [32] proposed a rejecting error scheme that can be implemented probabilistically based on parity check. Kalamidas [33] proposed a single-photon error-rejection scheme with the success probability 100 %, in which fast polarization modulator (Pockels cells) adds the operational difficulties. With an auxiliary photon in a fixed polarization state and deterministic two-qubit operation, Yamamoto et al. [34] proposed a protocol resisting collective noise with the probability 12.5 %. Employing only passive linear optical elements, the scheme in [35] can be realized with probability 50 %.

Invoking the Bell state and linear optics, Wang [36] proposed a quantum error-rejection scheme based on the idea of the quantum error correction code where only three qubits are required to correct error. The scheme requires a postselection measurement for collective respondence of three outlets, and the corresponding experiment was performed in [37]. Similar to BB84, the two-qubit QKD scheme proposed in [38] can tolerate error rate up to 26 % if only symmetric and independent errors occur on the individual qubit. Without collective quantum measurement or quantum memory, Wang [39] proposed a QKD scheme to countercheck an arbitrary collective unitary noise. Due to the parity check, these schemes are only implemented with probability.

When the noise shows some symmetry, regardless of its strength and weakness, there exist some quantum states that are invariant under this kind of noise and can be applied to protect quantum information. The Hilbert space with this property is called a decoherence-free subspace (DFS); it can be extended by many other degrees of freedom (DOFs), such as the time DOF [40–42], the spatial DOF [43–46], and the frequency DOF [47, 48].

Using the phase–time entanglement between two photons, Walton et al. [40] proposed a QKD scheme against dephasing noise. With the tag operation for encoding (time delay of one of the polarization modes), Boileau et al. [41] proposed a communication protocol without a shared spatial reference frame and precise timing. A corresponding experiment was completed in [42]. By changing the order of transmitting photons, the authors of [43] presented the schemes with three or four photons to remove the collective rotation noise. Similarly, the spatial DOF was used to obviate the collective noise [44–46]. Using the frequency DOF, a fault-tolerant communication with the probability 50 % was proposed in [48]. Moreover, the orbital angular momentum DOF [49] and the transverse spatial mode DOF [50] can also be used to realize communication.

With four-photon states, Bourennane et al. [51] proposed a scheme to transmit one-bit secret information for overcoming the rotation error. Considering the practical implementations of QKD scheme in DFS, a decoy method is proposed in [52] to keep off the photon-number-splitting attack.

In an ideal quantum channel, there exist some multi-user QKD protocols [13–16] in which the participants are introduced to control the communication process between senders and receivers. A secure and efficient controlled QKD scheme with refined data analysis was proposed in [15], in which the controller transmits two particles in a GHZ state to two communicators and retains one.

In this paper, taking collective noise into account, we propose two controlled quantum key distribution protocols in which the sender transmits two photons in a three-photon entangled state as a unit through the controller to the receiver and a one-bit secret key can be generated. The two explicit protocols against collective dephasing noise or collective rotation noise are presented in Sec. 2. In Sec. 3, we analyze the security of the above QKD protocols. Our work is concluded with the discussion and summary in Sec. 4.

2. CONTROLLED QUANTUM KEY DISTRIBUTION PROTOCOLS AGAINST COLLECTIVE DEPHASING NOISE OR COLLECTIVE ROTATION NOISE

An arbitrary collective random unitary noise on the transmission photons in the polarization state can be written as [39]

$$\begin{aligned} U\,|H\rangle &= \cos\theta\,|H\rangle + e^{i\phi}\sin\theta\,|V\rangle\,, \\ U\,|V\rangle &= e^{i(\Delta-\phi)}(-\sin\theta\,|H\rangle + e^{i\phi}\cos\theta\,|V\rangle), \end{aligned} \tag{2}$$

where $|H\rangle$ ($|V\rangle$) is the horizontal (vertical) polarization state. In general, it is not a method to make a unitary compensation on each photon in a transmission sequence because the noise parameters Δ, ϕ, and θ on the different photons fluctuate with time asynchronously. But the situation may be different if two or more qubits are considered simultaneously, that is, the collective assumption is introduced, and hence a fault-tolerant communication can be realized.

We first consider a special example where the channel noise mainly originates in the collective dephasing noise, that is, the parameter θ is equal to zero and the parameter ϕ is not restricted, and hence the effect of the noise on a polarization photon is given by

$$|H\rangle \xrightarrow{U_{cdn}} |H\rangle, \quad |V\rangle \xrightarrow{U_{cdn}} e^{i\phi}|V\rangle. \tag{3}$$

It is well known that three-particle entangled states can be classified into two classes, the GHZ and W states [53], which are inequivalent because they cannot be converted to each other under stochastic local operations and classical communication. We can perform a controlled quantum key distribution against collective dephasing noise.

There are four GHZ states that can circumvent collective dephasing noise if photons $\{B_1, B_2\}$ pass through the equal distance in the quantum channel:

$$\begin{aligned} |\Phi_1\rangle &= \frac{1}{\sqrt{2}}(|HHV\rangle + |VVH\rangle)_{AB_1B_2} = \\ &= \frac{1}{2}(|+++\rangle - |+--\rangle + |-+-\rangle - \\ &\qquad - |--+\rangle)_{AB_1B_2}, \\ |\Phi_2\rangle &= \frac{1}{\sqrt{2}}(|HHV\rangle - \\ &\qquad - |VVH\rangle)_{AB_1B_2} = \\ &= \frac{1}{2}(|++-\rangle - |+-+\rangle + |-++\rangle - \\ &\qquad - |---\rangle)_{AB_1B_2}, \\ |\Phi_3\rangle &= \frac{1}{\sqrt{2}}(|HVH\rangle + |VHV\rangle)_{AB_1B_2} = \\ &= \frac{1}{2}(|+++\rangle - |+--\rangle + |--+\rangle - \\ &\qquad - |-+-\rangle)_{AB_1B_2}, \\ |\Phi_4\rangle &= \frac{1}{\sqrt{2}}(|HVH\rangle - \\ &\qquad - |VHV\rangle)_{AB_1B_2} = \\ &= \frac{1}{2}(|+-+\rangle - |++-\rangle + |-++\rangle - \\ &\qquad - |---\rangle)_{AB_1B_2}, \end{aligned} \tag{4}$$

where

$$|+\rangle = \frac{1}{\sqrt{2}}\left(|H\rangle + |V\rangle\right), \quad |-\rangle = \frac{1}{\sqrt{2}}\left(|H\rangle - |V\rangle\right).$$

The participants can select any two of the above states to perform controlled QKD to overcome collective dephasing noise. We suppose that the sender, Alice, wishes to share a secret key with the receiver, Bob, in the charge of a controller, Charlie.

1. Alice prepares a large number of GHZ states expressed by Eq. (4), whose number is larger than the binary key length. Without loss of generality, we suppose that they are in the state $|\Phi_1\rangle$. She puts these photons into two sequences. One is the A sequence (photons $\{A\}$) and the other is the B sequence (photons $\{B_1, B_2\}$). Alice keeps the A sequence and sends the B sequence to Charlie.

2. After the receipt of the B sequence, Charlie performs control operations (unitary transformations U_i ($i = 1, 2$)) on each photon pair randomly, where

$$U_1 = I_{B_1} \otimes I_{B_2}, \quad U_2 = (\sigma_z)_{B_1} \otimes I_{B_2}, \tag{5}$$

which can change the original states as

$$U_1\,|\Phi_1\rangle = |\Phi_1\rangle\,, \quad U_2\,|\Phi_1\rangle = |\Phi_2\rangle\,. \tag{6}$$

Then Charlie randomly selects some photon pairs as the checking photons and sends the other photons to Bob.

3. Charlie checks the security of the distribution process between Alice and himself; this is the first security check. He randomly performs the $\{|H\rangle, |V\rangle\} \otimes \otimes \{|H\rangle, |V\rangle\}$ basis or the $\{|+\rangle, |-\rangle\} \otimes \{|+\rangle, |-\rangle\}$ basis measurements on the checking photons, and announces the position and the measurement bases, after which Alice performs measurements using the same bases on the corresponding photons and announces the measurement results. If their measurement results comply with Eq. (4), there is no eavesdropping on the line. Otherwise, they abandon and restart.

4. After receiving the B sequence, Bob randomly performs the $\{|H\rangle, |V\rangle\} \otimes \{|H\rangle, |V\rangle\}$ basis or the $\{|+\rangle, |-\rangle\} \otimes \{|+\rangle, |-\rangle\}$ basis measurements on each photon pair and registers the measurement results.

5. Alice, Bob, and Charlie check the security of the whole distribution process, which is the second security check. Bob selects a subset of the B sequence as checking photons, and the other photons are used as message photons. After Bob announces the position and the measurement bases of the checking photons, Charlie announces his unitary operations on them. Then Alice performs the measurement using the bases chosen by Bob on checking photons and announces the measurement results. According to Eqs. (4) and (6), Bob deduces the states of the checking photons, and compares their measurement results on them to judge whether the quantum channel is secure.

6. If the distribution process is secure, Alice and Bob commence to generate a secret key using the message photons. If Charlie agrees to the communication between Alice and Bob, the information with reference to control operations is offered to Bob. After Bob announces the instruction about her measurement basis (either the $\{|H\rangle, |V\rangle\}$ basis or the $\{|+\rangle, |-\rangle\}$ basis), Alice performs measurements. Consequently, she obtains the secret key according to her measurement results, with $|H\rangle$ ($|+\rangle$) corresponding to secret key "0" and $|V\rangle$ ($|-\rangle$) corresponding to secret key "1". Based on Charlie's information and his own measurement results, Bob can deduce Alice's measurement results and extract the secret key shared with Alice.

As an example, a six-bit secret key generation process via the collective dephasing noise channel is illustrated in Table 1, where the process of security check is not considered.

In the other case, for the quantum communication in free space, the dispersion of the transmitted photons may be small. Moreover, all elements in unitary noise can be considered real numbers and the rotation angle θ, the swinging angle, may be large and random. In the extreme case, we let $\phi = 0$ and call the noise model the collective rotation noise; its effect on the polarization state can be expressed as

$$\begin{aligned} |H\rangle &\xrightarrow{U_{crn}} \cos\theta|H\rangle + \sin\theta|V\rangle, \\ |V\rangle &\xrightarrow{U_{crn}} -\sin\theta|H\rangle + \cos\theta|V\rangle. \end{aligned} \tag{7}$$

The following four W states can be applied to circumvent collective rotation noise when photons $\{B_1, B_2\}$ pass through the equal distance of a quantum channel:

$$\begin{aligned} |\Psi_1\rangle &= \frac{1}{\sqrt{2}}(|H\rangle\,|\phi^+\rangle + |V\rangle\,|\psi^-\rangle)_{AB_1B_2} = \\ &= \frac{1}{2}[|+\rangle\,(|+\rangle\,|V\rangle + |-\rangle\,|H\rangle) + |-\rangle\,(|+\rangle\,|H\rangle - \\ &\qquad - |-\rangle\,|V\rangle)]_{AB_1B_2}, \\ |\Psi_2\rangle &= \frac{1}{\sqrt{2}}(|H\rangle\,|\phi^+\rangle - \\ &\qquad - |V\rangle\,|\psi^-\rangle)_{AB_1B_2} = \\ &= \frac{1}{2}[|+\rangle\,(|+\rangle\,|H\rangle - |-\rangle\,|V\rangle) + |-\rangle\,(|+\rangle\,|V\rangle + \\ &\qquad + |-\rangle\,|H\rangle)]_{AB_1B_2}, \\ |\Psi_3\rangle &= \frac{1}{\sqrt{2}}(|H\rangle\,|\psi^-\rangle + \\ &\qquad + |V\rangle\,|\phi^+\rangle)_{AB_1B_2} = \\ &= \frac{1}{2}[|+\rangle\,(|+\rangle\,|V\rangle + |-\rangle\,|H\rangle) + |-\rangle\,(|-\rangle\,|V\rangle - \\ &\qquad - |+\rangle\,|H\rangle)]_{AB_1B_2}, \\ |\Psi_4\rangle &= \frac{1}{\sqrt{2}}(|H\rangle\,|\psi^-\rangle - \\ &\qquad - |V\rangle\,|\phi^+\rangle)_{AB_1B_2} = \\ &= \frac{1}{2}[|+\rangle\,(|-\rangle\,|V\rangle - |+\rangle\,|H\rangle) + |-\rangle\,(|+\rangle\,|V\rangle + \\ &\qquad + |-\rangle\,|H\rangle)]_{AB_1B_2}. \end{aligned} \tag{8}$$

Alice and Bob can extract the secret key using steps similar to the above ones. But there are some differences. First, for circumventing the collective rotation noise, the state $|\Psi_1\rangle$ in Eq. (8) is prepared by the participants. Second, the unitary operations

$$U_1 = I_{B_1} \otimes I_{B_2}, \quad U_2 = (\sigma_z)_{B_1} \otimes (\sigma_z)_{B_2}, \tag{9}$$

are performed by Charlie to control the communication. Finally, after receiving the B sequence, Bob randomly performs the Bell basis or the $\{|+\rangle, |-\rangle\} \otimes \otimes \{|H\rangle, |V\rangle\}$ basis measurements on each photon pair to check the security or obtain the secret key (instead of the $\{|H\rangle, |V\rangle\} \otimes \{|H\rangle, |V\rangle\}$ basis or the $\{|+\rangle, |-\rangle\} \otimes \{|+\rangle, |-\rangle\}$ basis in a collective dephasing noise channel).

Table 1. Example of a six-bit secret key generation process via a collective dephasing noise channel

The state prepared by Alice	$\vert\Phi_1\rangle$	$\vert\Phi_1\rangle$	$\vert\Phi_1\rangle$	$\vert\Phi_1\rangle$	$\vert\Phi_1\rangle$	$\vert\Phi_1\rangle$
Charlie's control operation	U_1	U_2	U_2	U_1	U_2	U_1
The state between Alice and Bob	$\vert\Phi_1\rangle$	$\vert\Phi_2\rangle$	$\vert\Phi_2\rangle$	$\vert\Phi_1\rangle$	$\vert\Phi_2\rangle$	$\vert\Phi_1\rangle$
Bob's measurement basis	$++$	$\times\times$	$++$	$\times\times$	$\times\times$	$++$
Bob's measurement result	$\vert HV\rangle$	$\vert +-\rangle$	$\vert VH\rangle$	$\vert --\rangle$	$\vert ++\rangle$	$\vert VH\rangle$
Alice's measurement basis	$+$	$\times$	$+$	$\times$	$\times$	$+$
Alice's measurement result	$\vert H\rangle$	$\vert +\rangle$	$\vert V\rangle$	$\vert +\rangle$	$\vert -\rangle$	$\vert V\rangle$
The secret key	0	0	1	0	1	1

Bob's measurement basis "++" represents the $\{|H\rangle, |V\rangle\} \otimes \{|H\rangle, |V\rangle\}$ basis; "××" represents the $\{|+\rangle, |-\rangle\} \otimes \otimes \{|+\rangle, |-\rangle\}$ basis; Alice's measurement basis "+" represents the $\{|H\rangle, |V\rangle\}$ basis; and "×" represents the $\{|+\rangle, |-\rangle\}$ basis.

Table 2. Example of a six-bit secret key generation process via a collective rotation noise channel

The state prepared by Alice	$\vert\Psi_1\rangle$	$\vert\Psi_1\rangle$	$\vert\Psi_1\rangle$	$\vert\Psi_1\rangle$	$\vert\Psi_1\rangle$	$\vert\Psi_1\rangle$
Charlie's control operation	U_1	U_2	U_2	U_1	U_2	U_1
The state between Alice and Bob	$\vert\Psi_1\rangle$	$\vert\Psi_2\rangle$	$\vert\Psi_2\rangle$	$\vert\Psi_1\rangle$	$\vert\Psi_2\rangle$	$\vert\Psi_1\rangle$
Bob's measurement basis	Bell	$\times+$	Bell	$\times+$	$\times+$	Bell
Bob's measurement result	$\vert\phi^+\rangle$	$\vert +H\rangle$	$\vert\psi^-\rangle$	$\vert -H\rangle$	$\vert -H\rangle$	$\vert\psi^-\rangle$
Alice's measurement basis	$+$	$\times$	$+$	$\times$	$\times$	$+$
Alice's measurement result	$\vert H\rangle$	$\vert +\rangle$	$\vert V\rangle$	$\vert +\rangle$	$\vert -\rangle$	$\vert V\rangle$
The secret key	0	0	1	0	1	1

Bob's measurement basis "Bell" represents the Bell basis; "×+" represents the $\{|+\rangle, |-\rangle\} \otimes \{|H\rangle, |V\rangle\}$ basis; Alice's measurement basis "+" represents the $\{|H\rangle, |V\rangle\}$ basis; and "×" represents the $\{|+\rangle, |-\rangle\}$ basis.

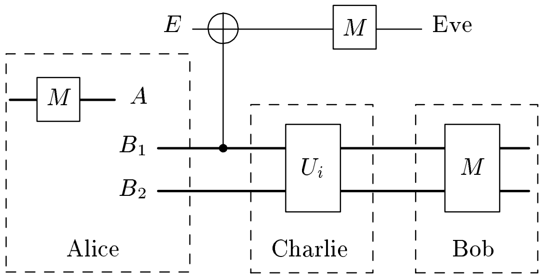

Fig. 1. The diagram describes the processes of communication between two participants and eavesdropper's wiretapping. A, B_1, and B_2 denote the photons in the entangled state at Alice's site originally. M denotes the measurement and U_i denotes the control operation

In Table 2, a generation instance of a six-bit secret key can be applied to interpret the decoding process via a collective rotation noise channel.

This protocol can be used to overcome the polarization rotation of transmitted photons. Moreover, it is unnecessary for the participants to share the same reference frame (e. g., a relative alignment of their linear polarizers), which can be realized via infinite turns in the quantum communication and consumes considerable resources. In Fig. 1, we depict an implementation circuit to illustrate this communication process via the collective noise channel.

3. SECURITY ANALYSIS OF THE CONTROLLED QUANTUM KEY DISTRIBUTION PROTOCOLS

We next discuss the security of the above distribution protocols from two standpoints. One is the eavesdropping action and the other is Bob's intention of denuding Charlie's control.

If an eavesdropper, Eve, wants to steal the secret key, she may adopt the methods as follows.

1. The intercept-resend-measure attack. Eve intercepts the photons transmitted to Charlie (Bob) and performs measurements on them, and then resends fake photons to Charlie (Bob), which are in the states she measured. Eve can obtain the secret key according to her measurement results and the publicized information from Bob and Charlie. In the first (second) security check process, if her measurement bases are the same as those selected by Charlie (Bob), Eve remains undetected. But if the measurement bases adopted by Eve and Charlie (Bob) are different, Eve's presence can be detected with the probability 50 %. Hence, the total detect probability is 25 %.

2. The intercept attack. Eve prepares photons $\{E_1, E_2, E_3\}$ in the entangled states in Eqs. (4) or (8). She intercepts and stores the transmitting photons $\{B_1, B_2\}$ from Alice, and sends photons $\{E_2, E_3\}$ to Charlie. After Charlie publicizes his unitary operations and Bob announces the measurement bases, Eve performs the measurements on photons $\{B_1, B_2\}$ and $\{E_1\}$. According to her measurement results on photons $\{B_1, B_2\}$ ($\{E_1\}$), Eve can share the secret key with Alice (Bob). It must be noted that the two sets of keys shared respectively by Alice–Eve and Bob–Eve are only identical with the probability $(1/2)^N$ (N is the number of secret keys).

However, the photons $\{E_2, E_3\}$ do not entangle with the photon $\{A\}$, and their measurement results are not correlated. Hence, in the first security check process, Eve is detected by Charlie with probability 50 %. If the eavesdropping attack is performed in the transmission path from Charlie to Bob, then Alice and Bob can detect it in the second security check process because the photons $\{E_2, E_3\}$ are not correlated with the photon $\{A\}$. Eve may construct the correlation of the photons $\{E_2, E_3, A\}$ by performing her operations on $\{B_1, B_2, E_1\}$, but this cannot guarantee that Alice and Bob obtain the measurement results associated with Eq. (4) or Eq. (8). Moreover, Eve cannot obtain the secret key of Alice and Bob by these methods.

3. The CNOT gate attack [54]. Eve introduces auxiliary photons and performs the CNOT gate operation on transmitted photons and auxiliary photons, whereby she obtains the secret key by measuring the auxiliary photons.

For the first protocol proposed in Sec. 2, Eve performs the CNOT gate operations C_{B_1E} shown in Fig. 1 on the photon $\{B_1\}$ and the photon $\{E\}$ that is in the state $|H\rangle$, where the photon $\{B_1\}$ acts as the control bit and $\{E\}$ acts as the target bit, which can be represented by

$$|B_1\rangle|E\rangle \xrightarrow{CNOT} |B_1\rangle|E \oplus B_1\rangle, \qquad (10)$$

in the computational basis. Afterwards, Eve performs an $\{|H\rangle, |V\rangle\}$ basis measurement on the photon $\{E\}$. It follows from Eq. (4) that the measurement results of Eve are always the same as Alice's in the basis of $\{|H\rangle, |V\rangle\}$.

For the second protocol in Sec. 2, Eve performs the CNOT gate operations C_{B_1E} and C_{B_2E} on the photons $\{B_1\}$, $\{B_2\}$, and an auxiliary photon $\{E\}$. In the basis of $\{|H\rangle, |V\rangle\}$, Eve's measurement results on the photon $\{E\}$ agree with Alice's, and hence Eve can obtain the same secret key as Alice.

In the first security check, if only an $\{|H\rangle, |V\rangle\}$ basis measurement is adopted by Alice and Charlie, Eve cannot be detected. But if the other checking basis, $\{|+\rangle, |-\rangle\}$, is used by Alice and Charlie, then Eve is detected with the probability 50 %. Hence, Eve is detected with the total probability 25 %. If Eve performs CNOT operations between Charlie and Bob, she is also detected with the total probability 25 % in the second security check.

On the other hand, if Bob wants to obtain the secret key without the permission of Charlie, he may adopt the following methods.

1. The intercept-measure method. Bob intercepts the transmitted photons from Alice to Charlie and makes measurements randomly on them in the $\{|H\rangle, |V\rangle\}$ or $\{|+\rangle, |-\rangle\}$ basis and registers the measurement results. Then he resends fake photons to Charlie. Bob can obtain Alice's secret key without the control of Charlie according to his measurement results. But in the first security check, Charlie finds that there is a 25 % error rate because the measurement bases of Bob and himself are only identical with 50 %. Therefore, he demands that Alice and Bob discard the secret key.

2. The CNOT gate method. Bob attempts to obtain Charlie's unitary operations by the CNOT gate method. For example, in the second protocol in Sec. 2, Bob introduces an auxiliary photon $\{E\}$ in the $|H\rangle$ state, and performs the CNOT gate operations C_{B_2E} twice, before and after the photon $\{B_2\}$ arrives to Charlie. Then he performs an $\{|H\rangle, |V\rangle\}$ basis measurement on the photon $\{E\}$. According to Eq. (8), in the basis $\{|+\rangle, |-\rangle\} \otimes \{|+\rangle, |-\rangle\} \otimes \{|H\rangle, |V\rangle\}$, if the unitary operation performed by Charlie is U_1, then Bob's measurement result is $|H\rangle$. If the unitary operation performed by Charlie is U_2, then Bob's measurement

result is $|V\rangle$. Therefore, Bob can obtain the secret key without the cooperation of Charlie. But during the first security check, Charlie then detects this with probability 25 % (a 50 % error rate in the Bell basis measurement and 0 % error rate in the $\{|+\rangle, |-\rangle\} \otimes \{|H\rangle, |V\rangle\}$ basis measurement). Consequently, Charlie informs Alice and announces that the process of sharing the secret key is invalid. The conclusion is similar in the first protocol.

Next, we consider the case where the two protocols are in different quantum noise channels, that is, the first protocol is in the collective rotation noise channel and the second protocol is in the collective dephasing noise channel. We let the probability that is not affected by the transmission path be denoted by p_0 and the affected one by p_e, with $p_0 + p_e = 1$.

In the first protocol, the quantum channel is immune to collective dephasing noise (U_{cdn}). But under the collective rotation noise (U_{crn}), it changes as

$$\begin{aligned}
&\frac{1}{\sqrt{2}}(|HHV\rangle + |VVH\rangle) \xrightarrow{U_{crn}} \frac{1}{\sqrt{2}} \times \\
&\quad \times \cos^2\theta(|HHV\rangle + |VVH\rangle) - \frac{1}{\sqrt{2}} \times \\
&\quad \times \sin^2\theta(|HVH\rangle + |VHV\rangle) - \\
&\quad - \frac{1}{\sqrt{2}} \sin\theta\cos\theta(|H\rangle + |V\rangle) \times \\
&\quad \times (|HH\rangle - |VV\rangle), \\
&\frac{1}{\sqrt{2}}(|HHV\rangle - |VVH\rangle) \xrightarrow{U_{crn}} \frac{1}{\sqrt{2}} \times \\
&\quad \times \cos^2\theta(|HHV\rangle - |VVH\rangle) - \\
&\quad - \frac{1}{\sqrt{2}} \sin^2\theta(|HVH\rangle - |VHV\rangle) - \\
&\quad - \frac{1}{\sqrt{2}} \sin\theta\cos\theta(|H\rangle - |V\rangle)(|HH\rangle - |VV\rangle),
\end{aligned} \tag{11}$$

and hence the channel error rate can be calculated as

$$P_{cer} = (1 - \cos^4\theta)p_e. \tag{12}$$

We now consider the key error rate and the key generation rate. For the first term in Eq. (11), the quantum channel is not changed, and hence there is no error. For the second term, according to Eq. (4), there is no error when the $\{|+\rangle, |-\rangle\}$ basis measurement is used, but a 100 % error is introduced when the $\{|H\rangle, |V\rangle\}$ basis measurement is selected. As regards the third term, a 100 % error is generated in both kinds of measurements. Therefore, the key error rate and the key generation rate are

$$\begin{aligned}
P_{ker} &= \left(1 - \cos^4\theta - \frac{1}{2}\sin^4\theta\right) p_e, \\
P_{kgr} &= 1 - \left(1 - \cos^4\theta - \frac{1}{2}\sin^4\theta\right) p_e.
\end{aligned} \tag{13}$$

In the second protocol, the quantum channel is not affected by the collective rotation noise (U_{crn}), but is affected by the collective dephasing noise (U_{cdn}):

$$\begin{aligned}
&\frac{1}{\sqrt{2}}(|H\rangle\,|\phi^+\rangle + |V\rangle\,|\psi^-\rangle) \xrightarrow{U_{cdn}} \\
&\xrightarrow{U_{cdn}} \frac{1}{\sqrt{2}} e^{i\phi}(\cos\phi\,|H\rangle\,|\phi^+\rangle - \\
&- i\sin\phi\,|H\rangle\,|\phi^-\rangle + |V\rangle\,|\psi^-\rangle) = \\
&= \frac{1}{4} e^{i\phi}[(e^{-i\phi} + 1)(|+-\rangle + |-+\rangle)\,|H\rangle + \\
&+ (e^{i\phi} + 1)(|++\rangle - |--\rangle)\,|V\rangle] + \\
&+ \frac{1}{4} e^{i\phi}[(e^{-i\phi} - 1)(|++\rangle + |--\rangle)\,|H\rangle - \\
&- (e^{i\phi} - 1)(|+-\rangle - |-+\rangle)\,|V\rangle], \\
&\frac{1}{\sqrt{2}}(|H\rangle\,|\phi^+\rangle - \\
&- |V\rangle\,|\psi^-\rangle) \xrightarrow{U_{cdn}} \frac{1}{\sqrt{2}} e^{i\phi}(\cos\phi\,|H\rangle\,|\phi^+\rangle - \\
&- i\sin\phi\,|H\rangle\,|\phi^-\rangle - |V\rangle\,|\psi^-\rangle) = \\
&= \frac{1}{4} e^{i\phi}[(e^{-i\phi} + 1)(|++\rangle + |--\rangle)\,|H\rangle - \\
&- (e^{i\phi} + 1)(|+-\rangle - |-+\rangle)\,|V\rangle] + \\
&+ \frac{1}{4} e^{i\phi}[(e^{-i\phi} - 1)(|+-\rangle + |-+\rangle)\,|H\rangle + \\
&+ (e^{i\phi} - 1)(|++\rangle - |--\rangle)\,|V\rangle].
\end{aligned} \tag{14}$$

Consequently, the channel error rate, the key error rate, and the key generation rate are given by

$$\begin{aligned}
P_{cer} &= \left[1 - \frac{1}{4}(1 + \cos\phi)^2\right] p_e, \\
P_{ker} &= \frac{1}{4}(1 - \cos\phi + \sin^2\phi)p_e, \\
P_{kgr} &= 1 - \frac{1}{4}(1 - \cos\phi + \sin^2\phi)p_e.
\end{aligned} \tag{15}$$

The channel error rate and the key generation rate of the two protocols in the opposite noise channel are depicted in Fig. 2. It can be seen that the key generation rates are high in both protocols when p_e is small or when p_e is large, but the noise parameters are $\theta \sim 0, \pi$ and $\phi \sim 0$. Therefore, the present protocol is workable when one kind of collective noise is dominant and the other is small.

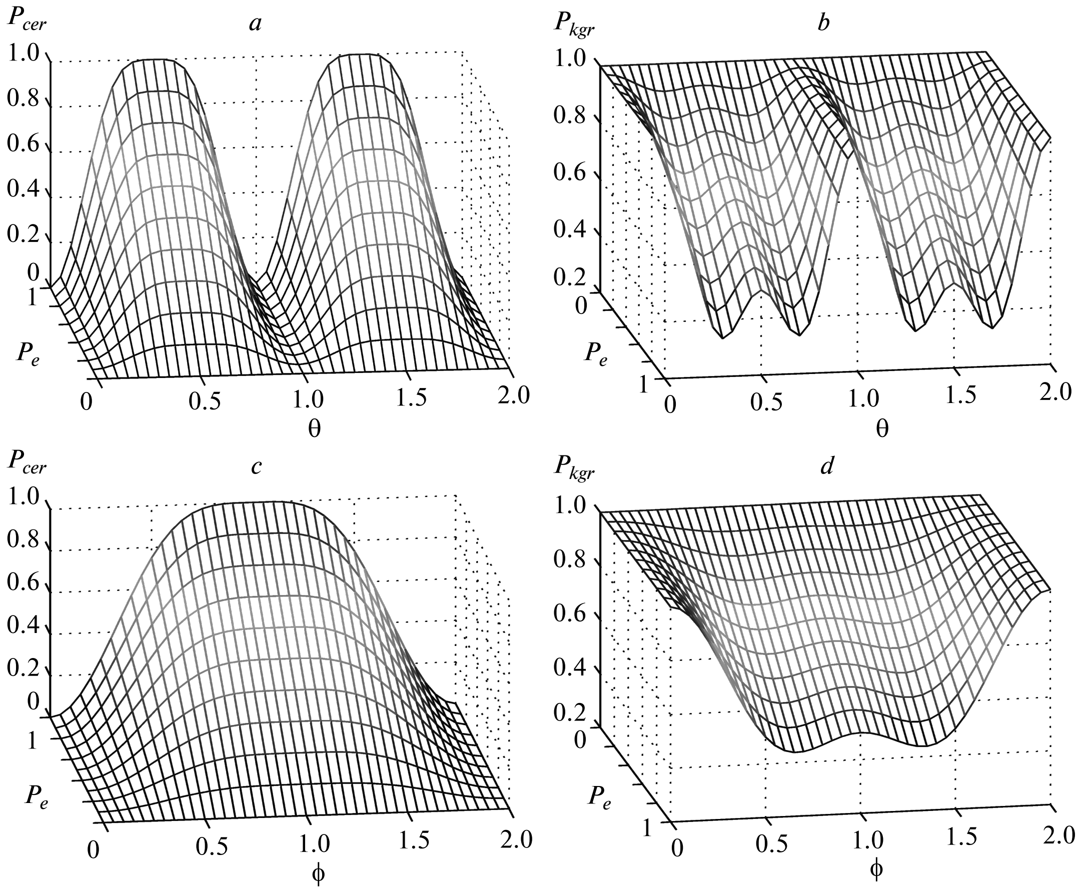

Fig. 2. The diagram depicting the channel error rate and the key generation rate of two protocols in the opposite noise channel. The angle θ (ϕ) with unit π is the noise parameter of collective rotation noise (collective dephasing noise). *a*: the channel error rate in the collective dephasing noise channel; *b*: the key generation rate in the collective dephasing noise channel; *c*: the channel error rate in the collective rotation noise channel; *d*: the key generation rate in the collective rotation noise channel

4. DISCUSSION AND SUMMARY

In this paper, we proposed the controlled QKD protocols for circumventing collective dephasing noise or collective rotation noise. In practical applications, the participants may attempt to solve it with a collective mode, in which a control switch is applied. They send auxiliary photons via the quantum channel (optical fiber or free space) to test the effects of collective dephasing noise and collective rotation noise. According to the test result, they determine which state should be applied to realize the communication and turn the switch to the corresponding process. With the collective method, this may weaken the effect of noise and improve the key generation rate. For instance, if the effect of collective dephasing noise is greater than that of collective rotation noise, the switch turns to the process of the first protocol, and vice versa.

We can increase the number of controllers by sending the transmitted photons to them. In contrast to the controlled communication protocols that need to change the number of entangled photons in the original state, Alice only needs to transmit a B sequence through all the controllers successively and require them to perform control operations, which can increase the number of the controllers. Independently of the number of the controllers, each three-photon entangled state can generate a one-bit secret key.

In these protocols, the receiver and the controller are not required to have a technique for storing photons, that is, they may operate on the photon pairs reaching them without delay. If the photon cost in the security check is not considered, the efficiencies of the two protocols in the corresponding noise channel are close to 100 %.

As a controller, Charlie cannot obtain the secret key but can demolish it. However, this action can be detected by Alice and Bob if they compare a part of the shared secret key.

In the above protocols, we only use the last two states in Eq. (4) or Eq. (8) to overcome the effect of the corresponding collective noise. If a controller performs the control operations

$$\begin{gathered} U_1 = I_{B_1} \otimes I_{B_2}, \quad U_2 = (\sigma_z)_{B_1} \otimes I_{B_2}, \\ U_3 = (\sigma_x)_{B_1} \otimes (\sigma_x)_{B_2}, \\ U_4 = (\sigma_x\sigma_z)_{B_1} \otimes (\sigma_x)_{B_2} \end{gathered} \tag{16}$$

in a collective dephasing noise channel or the control operations

$$\begin{gathered} U_1 = I_{B_1} \otimes I_{B_2}, \quad U_2 = (\sigma_z)_{B_1} \otimes (\sigma_z)_{B_2}, \\ U_3 = (\sigma_z)_{B_1} \otimes (\sigma_x)_{B_2}, \quad U_4 = I_{B_1} \otimes (\sigma_x\sigma_z)_{B_2} \end{gathered} \tag{17}$$

in a collective rotation noise channel, then they can change the original state prepared by Alice to the other states in Eq. (4) or Eq. (8). But this is invalid for increasing the number of secret bits, and is therefore dispensable.

This study was supported by the Research Program of the Educational Office of Liaoning Province of China (Grant No. 2008006). We thank the anonymous referees for constructive comments.

REFERENCES

1. C. H. Bennett and G. Brassard, in *Proc. IEEE Int. Conf. on Computer, Systems and Signal Processing*, Bangalore, India (IEEE, New York) 175 (1984).

2. C. H. Bennett, Phys. Rev. Lett. **68**, 3121 (1992).

3. A. K. Ekert, Phys. Rev. Lett. **67**, 661 (1991).

4. C. H. Bennett, G. Brassard, and N. D. Mermin, Phys. Rev. Lett. **68**, 557 (1992).

5. D. Bruß, Phys. Rev. Lett. **81**, 3018 (1998).

6. G. L. Long and X. S. Liu, Phys. Rev. A **65**, 032302 (2002).

7. F. G. Deng and G. L. Long, Phys. Rev. A **68**, 042315 (2003).

8. F. G. Deng and G. L. Long, Phys. Rev. A **70**, 012311 (2004).

9. W. Chen, Z. F. Han, X. F. Mo, F. X. Xu, G. Wei, and G. C. Guo, Chin. Sci. Bull. **53**, 1310 (2008).

10. H. Wen, Z. F. Han, Y. B. Zhao, G. C. Guo, and P. L. Hong, Sci. Chin. Ser. F **52**, 18 (2009).

11. K. Tamaki and G. Kato, Phys. Rev. A **81**, 022316 (2010).

12. A. R. Dixon, Z. L. Yuan, J. F. Dynes, A. W. Sharpe, and A. J. Shields, Appl. Phys. Lett. **96**, 161102 (2010).

13. S. Phoenix, S. Barnett, P. Townsend, and K. Blow, J. Mod. Opt. **42**, 1155 (1995).

14. P. Xue, C. F. Li, and G. C. Guo, Phys. Rev. A **65**, 022317 (2002).

15. C. Han, P. Xue, and G. C. Guo, Chin. Phys. Lett. **20**, 183 (2003).

16. F. Gao, S. J. Qin, F. Z. Guo, and Q. Y. Wen, arXiv:1009.2545.

17. A. V. Korol'kov, K. G. Katamadze, S. P. Kulik, and S. N. Molotkov, Zh. Eksp. Teor. Fiz. **137**, 637 (2010).

18. P. W. Shor, Phys. Rev. A **52**, R2493 (1995).

19. A. M. Steane, Phys. Rev. Lett. **77**, 793 (1996); Proc. Roy. Soc. London, Ser. A **452**, 2551 (1996).

20. C. H. Bennett, D. P. DiVincenzo, J. A. Smolin et al., Phys. Rev. A **54**, 3824 (1996); R. Laflamme, C. Miquel, J. P. Paz et al., Phys. Rev. Lett. **77**, 198 (1996).

21. C. H. Bennett, G. Brassard, S. Popescu, B. Schumacher, J. A. Smolin, and W. K. Wootters, Phys. Rev. Lett. **76**, 722 (1996).

22. D. Deutsch et al., Phys. Rev. Lett. **77**, 2818 (1996).

23. J. W. Pan, C. Simon, and A. Zellinger, Nature **410**, 1067 (2001).

24. C. Simon and J. W. Pan, Phys. Rev. Lett. **89**, 257901 (2002).

25. Y. B. Sheng, F. G. Deng, and H. Y. Zhou, Phys. Rev. A **77**, 042308 (2008); ibid. **77**, 062325 (2008); Y. B. Sheng and F. G. Deng, Phys. Rev. A **81**, 032307 (2010).

26. P. Zanardi and M. Rasetti, Phys. Rev. Lett. **79**, 3306 (1997).

27. J. D. Franson and B. C. Jacobs, Electron. Lett. **31**, 232 (1995).

28. P. Townsend, J. G. Rarity, and P. R. Tapster, Electron. Lett. **29**, 634 (1993).

29. M. Martinelli, Opt. Comm. **72**, 341 (1989); J. Mod. Opt. **39**, 451 (1992).

30. A. Muller et al., Appl. Phys. Lett. **70**, 793 (1997); D. Stucki, N. Ginsin, O. Guinnard, and H. Zbinden, New J. Phys. **4**, 41 (2002).

31. D. A. Kronberg and S. N. Molotkov, Zh. Eksp. Teor. Fiz. **138**, 33 (2010).

32. D. Bouwmeester, Phys. Rev. A **63**, 040301(R) (2001).

33. D. Kalamidas, Phys. Lett. A **321**, 87 (2004); **343**, 331 (2005).

34. T. Yamamoto, J. Shimamura, S. K. Özdemir, M. Koashi, and N. Imoto, Phys. Rev. Lett. **95**, 040503 (2005); T. Yamamoto, R. Nagase, J. Shimamura, S. K. Özdemir, M. Koashi, and N. Imoto, New J. Phys. **9**, 191 (2007).

35. X. H. Li, F. G. Deng, and H. Y. Zhou, Appl. Phys. Lett. **91**, 144101 (2007).

36. X. B. Wang, Phys. Rev. A **69**, 022320 (2004).

37. Y. A. Chen, A. N. Zhang, Z. Zhao, X. Q. Zhou, and J. W. Pan, Phys. Rev. Lett. **96**, 220504 (2006).

38. X. B. Wang, Phys. Rev. Lett. **92**, 077902 (2004).

39. X. B. Wang, Phys. Rev. A **72**, 050304(R) (2005).

40. Z. D. Walton, A. F. Abouraddy, A. V. Sergienko, B. E. A. Saleh, and M. C. Teich, Phys. Rev. Lett. **91**, 087901 (2003).

41. J. C. Boileau, R. Laflamme, M. Laforest, and C. R. Myers, Phys. Rev. Lett. **93**, 220501 (2004).

42. T. Y. Chen, J. Zhang, J. C. Boileau, X. M. Jin, Bin Yang, Q. Zhang, T. Yang, R. Laflamme, and J. W. Pan, Phys. Rev. Lett. **96**, 150504 (2006).

43. J. C. Boileau, D. Gottesman, R. Laflamme, D. Poulin, and R. W. Spekkens, Phys. Rev. Lett. **92**, 017901 (2004).

44. X. H. Li, F. G. Deng, and H. Y. Zhou, Phys. Rev. A **78**, 022321 (2008).

45. L. Dong, X. M. Xiu, Y. J. Gao, and F. Chi, Opt. Comm. **282**, 1688 (2009).

46. X. M. Xiu, L. Dong, Y. J. Gao, and F. Chi, Opt. Comm. **282**, 4171 (2009).

47. L. Xiao, C. Wang, W. Zhang, Y. D. Huang, J. D. Peng, and G. L. Long, Phys. Rev. A **77**, 042315 (2008).

48. X. H. Li, B. K. Zhao, Y. B. Sheng, F. G. Deng, and H. Y. Zhou, Opt. Comm. **282**, 4025 (2009).

49. L. Allen, M. W. Beijersbergen, R. J. C. Spreeuw, and J. P. Woerdman, Phys. Rev. A **45**, 8185 (1992).

50. L. Aolita and S. P. Walborn, Phys. Rev. Lett. **98** 100501 (2007); C. E. R. Souza and C. V. S. Borges, Phys. Rev. A **77**, 032345 (2008).

51. M. Bourennane, M. Eibl, S. Gaertner, C. Kurtsiefer, A. Cabello, and H. Weinfurter, Phys. Rev. Lett. **92**, 107901 (2004).

52. Z. Q. Yin, Y. B. Zhao, Z. W. Zhou, Z. F. Han, and G. C. Guo, Phys. Rev. A **77**, 062326 (2008).

53. W. Dür, G. Vidal, and J. I. Cirac, Phys. Rev. A **62**, 062314 (2000).

54. F. Gao, Q. Y. Wen, and F. C. Zhu, Phys. Lett. A **360**, 748 (2007); S. J. Qin, F. Gao, F. Z. Guo, and Q. Y. Wen, Phys. Rev. A **82**, 036301 (2010).