Blind quantum computation with a noise channel

Yu-Bo Sheng[1,3,*] and Lan Zhou[2,3]

[1]*Institute of Quantum Information and Technology, Nanjing University of Posts and Telecommunications, Nanjing 210003, China*

[2]*School of Science, Nanjing University of Posts and Telecommunications, Nanjing 210003, China*

[3]*Key Laboratory of Broadband Wireless Communication and Sensor Network Technology, Nanjing University of Posts and Telecommunications, Ministry of Education, Nanjing 210003, China*

(Received 19 March 2018; published 27 November 2018)

Blind quantum computation (BQC) is a type of quantum computation model. For a client (Alice) who does not have enough sophisticated technology and knowledge to perform universal quantum computation, BQC allows her to resort to a remote quantum computation server (Bob) to delegate universal quantum computation. During the computation, Bob cannot know Alice's inputs, algorithm, and outputs. A single-server BQC protocol requires Alice to prepare and distribute single-photon states to Bob. Unfortunately, the distributed single photons will suffer from noise. The noise not only leads to the decoherence of the single-photon state, but also leads to photon loss. In this protocol, we describe an antinoise single-server BQC protocol. This protocol has three advantages. First, Alice does not require any auxiliary resources, which reduces the client's economic cost. Second, this protocol not only can protect the state from the collective noise, but also can distill the single photon from photon loss. Third, the noise processer in Bob is based on the linear optics so that it is feasible in experiment. This protocol may show that it is possible to perform a single-server BQC protocol in a noise channel.

DOI: 10.1103/PhysRevA.98.052343

I. INTRODUCTION

Quantum computation has attracted much interest for its ultrafast computation ability. Shor's algorithm for integer factorization [1], Grover's algorithm, and the optimal Long algorithm for unsorted database search [2,3] have all displayed the great computing power of quantum computers. Small-scale quantum computers in ions [4], superconduction [5], and some other important quantum systems have been widely investigated [6]. It is not a dream to successfully produce a quantum computer in the foreseeable future. Like current supercomputers, the first generation of quantum computers must be very expensive and can be owned by very few governments or some big companies. As an ordinary quantum computer client, Alice has poor quantum ability and is insufficient to realize universal quantum computation. Blind quantum computation (BQC) provides her another quantum computation model. In BQC, Alice can resort to quantum computation servers (Bob) to perform universal quantum computation [7]. During the computation, Alice's inputs, algorithms, and outputs can be absolutely secure.

In 2005, Childs proposed the first BQC model [7]. It is the standard quantum circuit model. In the protocol, Bob needs to perform the quantum gates and Alice is required to have the quantum memory. In 2009, Broadbent, Fitzsimons, and Kashefi (BFK) proposed a BQC protocol based on the one-way quantum computation model [8]. In their protocol, Alice is only required to generate the single-qubit quantum state and have a classical computer. The greatest advantage of this protocol is that Alice does not need quantum memory. There are also some other important BQC protocols [9–27]. For example, Morimae *et al.* proposed two BQC protocols based on the Affleck-Kennedy-Lieb-Tasaki state [9]. Fitzsimons and Kashefi constructed a verifiable BQC protocol [11]. An experiment of the BFK protocol in an optical system was also reported [16]. Generally, these kinds of BQC protocols can be divided into three groups. The first group is the single-server BQC model [7–16,18–22,25]. The second group is double-server BQC model [8,17,24], and the third group is the triple-server BQC model [23].

In the single-server BQC protocol, Alice is required to have the quantum ability of generating and distributing the single quantum states. Certainly, Alice can perform single-qubit measurement with the approach of remote state preparation instead of state preparation. In the double-server BQC protocol, Alice can be completely classical and the two servers Bob1 and Bob2 should distribute and share nonlocal maximally entangled states. In the triple-sever BQC model, Alice is only required to receive and forward single qubits. Two of the three servers should share nonlocal maximally entangled states and the third server assists them to make the Bell state measurements. In practical applications, all three kinds of BQC protocols must consider imperfections. The first imperfection may come from the client's low quantum ability. For example, in current technology, the client does not have the ability to prepare ideal single photons. In order to solve this problem, Dunjko *et al.* first discussed the BQC model with practical weak coherent pulses [13]. The work of Ref. [13] was improved by introducing the decoy state method [27], which was widely used in the quantum key distribution system. They also discussed the security of the BQC model in a loss channel [13,27]. Another imperfection may come from the noise channel. In double-server BQC, Morimae and Fujii first described an efficient secure entanglement distillation for double-server BQC [17]. They showed

*shengyb@njupt.edu.cn

that it is possible to perform entanglement distillation in the double-server scheme without degrading the security of blind quantum computation. In 2015, we proposed deterministic entanglement distillation for secure double-server BQC [24]. In 2016, Takeuchi *et al.* first considered the model of single-server BQC over a collective-noise channel, which is called DFS-BQC [25]. They described three variations of DFS-BQC protocols, combined with the ideas based on decoherence-free subspace (DFS) and the BFK protocol. In this paper, we describe another antinoise single-sever BQC protocol based on the original BFK protocol [8]. Differently from previous DFS-BQC protocols, this protocol has some advantages. First, Alice is not required to generate Bell states or coherent light, but only to distribute and operate the single photons in linear optics, which reduces the client's technical difficulties and economic cost. Second, this protocol not only can protect the state from the collective noise, but also can distill the single photon from photon loss. Third, the noise processer in Bob is in linear optics and it is feasible for experiment.

This paper is organized as follows. In Sec. II, we will explain our antinoise single-server BQC protocol. In Sec. III, we will provide some discussion. In Sec. IV, we will present a conclusion.

II. BASIC MODEL OF ANTINOISE SINGLE-SERVER BQC PROTOCOL

Before we explain this protocol, we first briefly describe the original BFK protocol [8]. Suppose that Alice wants to perform one-way quantum computation with the m-qubit graph state G. The measurement basis is $\{|\bar{0}\rangle \pm e^{i\phi_j}|\bar{1}\rangle\}$. Here j is the jth qubit ($j = 1, 2, \ldots, m$) and $\phi_j \in \{k\pi/4 \mid k \in Z, 0 \leqslant k \leqslant 7\}$. It runs as follows [8,17]: (a) Client Alice first prepares n rotated qubits $\{|+_{\theta_j}\rangle \equiv (|\bar{0}\rangle + e^{i\theta_j}|\bar{1}\rangle)/\sqrt{2}\}_{j=1}^{m}$ and distributes them to the server Bob. Here $\theta_j \in \{k\pi/4 \mid k \in Z, 0 \leqslant k \leqslant 7\}$. (b) Bob prepares the graph state G, which Alice tells him. Here $|G\{\theta_j\}\rangle \equiv (\bigotimes_{i,j} \in E)CZ_{i,j} \bigotimes_{j=1}^{m} |\theta_j\rangle$. E is the set of edges of G, and $CZ_{i;j}$ is the controlled-Z gate between the ith and jth qubits. (c) Bob performs the measurement on the jth qubit according to measurement angle $\xi_j = \theta_j + \phi'_j + r_j\pi$, which Alice tells him. Here r_j is a random number and $r_j \in \{0, 1\}$. ϕ'_j is the modified version of ϕ_j according to the previous measurement results. (d) Bob sends the measurement results to Alice and Alice completes the computation with a classical computer.

The basic model of this antinoise BQC protocol is shown in Fig. 1. On the side of Alice, Alice first prepares n rotated qubits $\{|+_{\theta_j}\rangle \equiv (|\bar{0}\rangle + e^{i\theta_j}|\bar{1}\rangle)/\sqrt{2}\}_{j=1}^{n}$. In an optical system, we denote the horizontally polarized photon $|H\rangle$ as $|\bar{0}\rangle$ and vertically polarized photon $|V\rangle$ as $|\bar{1}\rangle$. In the traditional BFK protocol, the single-photon state $|+_{\theta_j}\rangle$ is sent to Bob directly. In this protocol, Alice first encodes the state $|+_{\theta_j}\rangle$ as shown in Fig. 2 to be [28]

$$\begin{aligned}|+_{\theta_j}\rangle &= \frac{1}{\sqrt{2}}(|H\rangle + e^{i\theta_j}|V\rangle) \to \frac{1}{\sqrt{2}}(|H_S\rangle + e^{i\theta_j}|H_L\rangle)\\ &\to \frac{1}{2}(|H_S\rangle_{a_1} + e^{i\theta_j}|H_L\rangle_{a_1}) + \frac{1}{2}(|H_S\rangle_{b_1} - e^{i\theta_j}|H_L\rangle_{b_1}).\end{aligned} \tag{1}$$

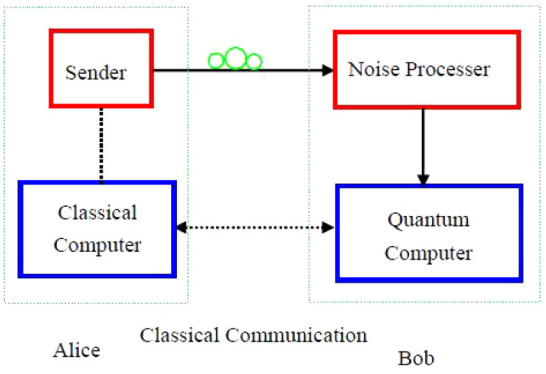

FIG. 1. Schematic of the antinoise BQC protocol. Alice prepares and encodes the single-photon state $|+_{\theta_j}\rangle$ to resist the collective noise in the sender. Bob distills the polluted single-photon state using the noise processer, before starting the BQC protocol.

The photon will suffer from noise, which will make

$$|H\rangle_{a_1} \to \alpha|H\rangle_{a_1} + \beta|V\rangle_{a_1} \tag{2}$$

and

$$|H\rangle_{b_1} \to \tau|H\rangle_{b_1} + \delta|V\rangle_{b_1}. \tag{3}$$

Here $|\alpha|^2 + |\beta|^2 = 1$ and $|\tau|^2 + |\delta|^2 = 1$. a_1 and b_1 are the spatial modes as shown in Fig. 2. PBS is the polarization beam splitter which can transmit the horizontally polarized photon and reflect the vertically polarized photon. BS is the 50:50 beam splitter. The photon in $|H\rangle$ will pass through the short (S) path and $|V\rangle$ will pass through the long (L) path. The noise model is called the collective noise model [25,28–34]. Therefore, after transmission, if the photon is not lost, the state $|+_{\theta_j}\rangle$ becomes

$$\begin{aligned}|+_{\theta_j}\rangle \to |+_{\theta_j}\rangle' = \tfrac{1}{2}[&(\alpha|H_S\rangle_{a_1} + \beta|V_S\rangle_{a_1})\\ &+ e^{i\theta_j}(\alpha|H_L\rangle_{a_1} + \beta|V_L\rangle_{a_1})]\\ &+ \tfrac{1}{2}[(\tau|H_S\rangle_{b_1} + \delta|V_S\rangle_{b_1})\\ &- e^{i\theta_j}(\tau|H_L\rangle_{b_1} + \delta|V_L\rangle_{b_1})].\end{aligned} \tag{4}$$

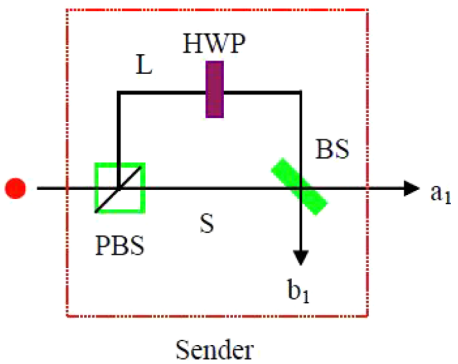

FIG. 2. Schematic of the sender as shown in Fig. 1. The sender is composed of a PBS, a BS, and an HWP. BS is the 50:50 beam splitter and PBS is the polarization beam splitter. HWP is the half-wave plate which can convert the $|H\rangle$ polarized photon to the $|V\rangle$ polarized photon and vice versa. The photon in $|H\rangle$ will pass through the short (S) path and $|V\rangle$ will pass through the long (L) path.

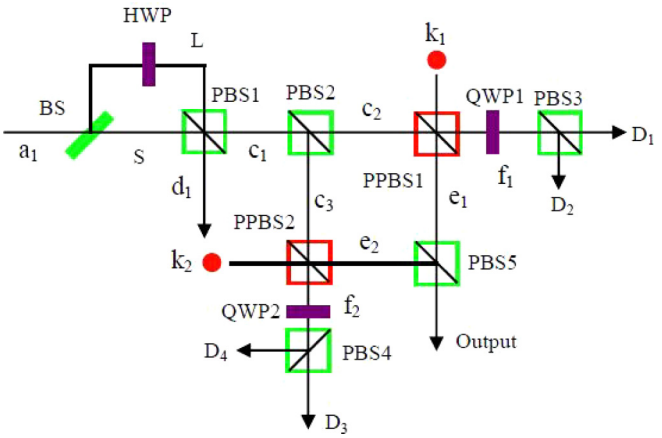

FIG. 3. Schematic of the noise processer as shown in Fig. 1. Bob requires the polarized Bell state in k_1k_2 spatial modes as auxiliary. QWP is the quarter-wave plate which acts as the Hadamard operation. PPBS is the partial-polarization beam splitter.

Certainly, the single-photon state $|+_{\theta_j}\rangle$ may also suffer from the photon loss. Generally, Bob will receive a mixed state ρ_{θ_j}, which can be written as

$$\rho_{\theta_j} = F|+_{\theta_j}\rangle''\langle+_{\theta_j}|+(1-F)|0\rangle\langle 0|. \tag{5}$$

Here F denotes the transmission efficiency of the photon. $|0\rangle$ is the Fock state which means no photon. As the transmission efficiency is usually decided by the length of transmittance, we suppose that the transmission efficiency in spatial modes a_1 and b_1 is the same. From Eq. (5), before Bob starts the BQC protocol, he should distill the mixed state ρ_{θ_j} and obtain the original state $|+_{\theta_j}\rangle$ deterministically. The noise processer shown in Fig. 1 is to complete the task. From Eq. (4), if the single photon is not lost, it will be in the spatial mode a_1 or b_1 with equal probability of 50%. The noise processer in Fig. 3 shows the detailed distillation process in spatial mode a_1. If the photon is in spatial mode b_1, Bob can also distill it with the same setup. We take the photon in spatial mode a_1 for example. As shown in Fig. 3, the quantum state can evolve as

$$\begin{aligned}
&(\alpha|H_S\rangle_{a_1} + \beta|V_S\rangle_{a_1}) + e^{i\theta_j}(\alpha|H_L\rangle_{a_1} + \beta|V_L\rangle_{a_1}) \\
&\quad\to \frac{1}{\sqrt{2}}(\alpha|H_{SS}\rangle + \alpha|V_{SL}\rangle + \beta|H_{SL}\rangle + \beta|V_{SS}\rangle) \\
&\qquad + \frac{1}{\sqrt{2}}e^{i\theta_j}(\alpha|H_{LS}\rangle + \alpha|V_{LL}\rangle + \beta|H_{LL}\rangle + \beta|V_{LS}\rangle) \\
&\quad= \frac{1}{\sqrt{2}}(\alpha|H_{SS}\rangle_{c_1} + \alpha|V_{SL}\rangle_{c_1} + \beta|H_{SL}\rangle_{d_1} + \beta|V_{SS}\rangle_{d_1}) \\
&\qquad + \frac{1}{\sqrt{2}}e^{i\theta_j}(\alpha|H_{LS}\rangle_{c_1} + \alpha|V_{LL}\rangle_{c_1} \\
&\qquad + \beta|H_{LL}\rangle_{d_1} + \beta|V_{LS}\rangle_{d_1}) \\
&\quad= \frac{\alpha}{\sqrt{2}}(e^{i\theta_j}|H_{LS}\rangle_{c_1} + |V_{SL}\rangle_{c_1}) \\
&\qquad + \frac{\beta}{\sqrt{2}}(|H_{SL}\rangle_{d_1} + e^{i\theta_j}|V_{LS}\rangle_{d_1})
\end{aligned}$$

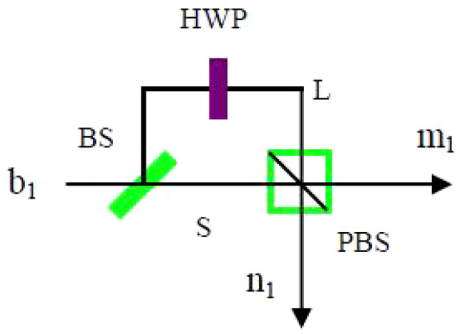

FIG. 4. Schematic of decoding if the single photon is in the spatial mode b_1.

$$\begin{aligned}
&+ \frac{1}{\sqrt{2}}(\alpha|H_{SS}\rangle_{c_1} + \beta|V_{SS}\rangle_{d_1}) \\
&+ \frac{1}{\sqrt{2}}e^{i\theta_j}(\alpha|V_{LL}\rangle_{c_1} + \beta|H_{LL}\rangle_{d_1}).
\end{aligned} \tag{6}$$

From Eq. (6), if the photon is not lost, it will be in a different arriving time, i.e., SS, LS (SL), or LL. Therefore, Bob can get the uncorrupted states $|-_{\theta_j}\rangle$ in spatial mode c_1, or $|+_{\theta_j}\rangle$ in spatial mode d_1 in the determinate time corresponding to SL and LS. Here $|-_{\theta_j}\rangle = e^{i\theta_j}|H\rangle + |V\rangle$. One can perform a bit-flip operation $\sigma_x = |H\rangle\langle V| + |V\rangle\langle H|$ to convert $|-_{\theta_j}\rangle$ to $|+_{\theta_j}\rangle$. From Eq. (4), if the single photon is in the spatial mode b_1, Bob can deal with it with the same principle, using BS, the half-wave plate (HWP), and PBS. Therefore, if the photon does not lose, Bob will finally obtain a single-photon entangled state in the time bin SL (LS) as

$$\begin{aligned}
|\varphi\rangle = &\frac{\alpha}{\sqrt{2}}\big|+_{\theta_j}\big\rangle_{c_1}|0\rangle_{d_1}|0\rangle_{m_1}|0\rangle_{n_1} \\
&+ \frac{\beta}{\sqrt{2}}|0\rangle_{c_1}\big|+_{\theta_j}\big\rangle_{d_1}|0\rangle_{m_1}|0\rangle_{n_1} \\
&+ \frac{\tau}{\sqrt{2}}|0\rangle_{c_1}|0\rangle_{d_1}\big|+_{\theta_j}\big\rangle_{m_1}|0\rangle_{n_1} \\
&+ \frac{\delta}{\sqrt{2}}|0\rangle_{c_1}|0\rangle_{d_1}|0\rangle_{m_1}\big|+_{\theta_j}\big\rangle_{n_1}.
\end{aligned} \tag{7}$$

Here the spatial modes m_1 and n_1 are shown in Fig. 4. This means that if the photon is in the spatial mode b_1 as shown in Fig. 2, Bob can deal with the collective noise with the setup of Fig. 4.

Combined with the case of photon loss, by selecting the time bin SL (LS), the state in Eq. (5) can be rewritten as

$$\rho'_{\theta_j} = F|\varphi\rangle\langle\varphi|+(1-F)|0\rangle\langle 0|. \tag{8}$$

From Eq. (8), the next step of Bob is to distill $|\varphi\rangle$ from the mixed state deterministically. Here we exploit the linear noiseless amplification (NLA) to complete the task [35]. We introduce a pair of ancillary polarized photons of the form

$$|\phi_1\rangle = \frac{1}{\sqrt{2}}\big(|H\rangle_{k_1}|H\rangle_{k_2} + |V\rangle_{k_1}|V\rangle_{k_2}\big). \tag{9}$$

Here the subscripts k_1 and k_2 are the spatial modes as shown in Fig. 3. The partial-polarization beam splitter PPBS1 can reflect the vertically polarized photon totally, while reflecting

the horizontally polarized photon with a coefficient of γ and transmitting it with a coefficient of $\sqrt{1-\gamma^2}$. PPBS2 can reflect the horizontally polarized photon totally, while reflecting the vertically polarized photon with the coefficient γ and transmitting it with a coefficient of $\sqrt{1-\gamma^2}$. For instance, PPBS1 can make [35]

$$\begin{aligned}
&\hat{a}^{\dagger}_{c_1,H}|0\rangle \rightarrow \gamma\hat{a}^{\dagger}_{e_1,H}|0\rangle + \sqrt{1-\gamma^2}\hat{a}^{\dagger}_{f_1,H}|0\rangle,\\
&\hat{a}^{\dagger}_{k_1,H}|0\rangle \rightarrow -\gamma\hat{a}^{\dagger}_{f_1,H}|0\rangle + \sqrt{1-\gamma^2}\hat{a}^{\dagger}_{e_1,H}|0\rangle,\\
&\hat{a}^{\dagger}_{k_1,V}|0\rangle \rightarrow -\hat{a}^{\dagger}_{f_1,V}|0\rangle. \qquad (10)
\end{aligned}$$

Here $\hat{a}^{\dagger}$ is the creation operator. The subscripts c_1, f_1, and e_1 are the spatial modes as shown in Fig. 3. Therefore, by selecting the successful amplification case that the spatial modes f_1 and f_2 both exactly contain one photon, we can obtain the relationship as follows:

$$\begin{aligned}
|0_{c_1}H_{k_1}H_{k_2}\rangle &\rightarrow \frac{\gamma}{2}|0_{\text{out}}\rangle\big(|H_{D_1}H_{D_3}\rangle + |H_{D_1}V_{D_4}\rangle\\
&\quad + |V_{D_2}H_{D_3}\rangle + |V_{D_2}V_{D_4}\rangle\big),\\
|0_{c_1}V_{k_1}V_{k_2}\rangle &\rightarrow \frac{\gamma}{2}|0_{\text{out}}\rangle\big(|H_{D_1}H_{D_3}\rangle - |H_{D_1}V_{D_4}\rangle\\
&\quad - |V_{D_2}H_{D_3}\rangle + |V_{D_2}V_{D_4}\rangle\big),\\
|H_{c_1}H_{k_1}H_{k_2}\rangle &\rightarrow \frac{(2\gamma^2-1)}{2}|H_{\text{out}}\rangle\big(|H_{D_1}H_{D_3}\rangle + |H_{D_1}V_{D_4}\rangle\\
&\quad + |V_{D_2}H_{D_3}\rangle + |V_{D2}V_{D4}\rangle\big),\\
|H_{c_1}V_{k_1}V_{k_2}\rangle &\rightarrow \frac{\gamma^2}{2}|H_{\text{out}}\rangle\big(|H_{D_1}H_{D_3}\rangle - |H_{D_1}V_{D_4}\rangle\\
&\quad - |V_{D_2}H_{D_3}\rangle + |V_{D_2}V_{D_4}\rangle\big),\\
|V_{c_1}H_{k_1}H_{k_2}\rangle &\rightarrow \frac{\gamma^2}{2}|V_{\text{out}}\rangle\big(|H_{D_1}H_{D_3}\rangle + |H_{D_1}V_{D_4}\rangle\\
&\quad + |V_{D_2}H_{D_3}\rangle + |V_{D_2}V_{D_4}\rangle\big),\\
|V_{c_1}V_{k_1}V_{k_2}\rangle &\rightarrow \frac{(2\gamma^2-1)}{2}|V_{\text{out}}\rangle\big(|H_{D_1}H_{D_3}\rangle - |H_{D_1}V_{D_4}\rangle\\
&\quad - |V_{D_2}H_{D_3}\rangle + |V_{D_2}V_{D_4}\rangle\big). \qquad (11)
\end{aligned}$$

For example, after the PPBSs, the first item $|0_{c_1}H_{k_1}H_{k_2}\rangle$ evolves as

$$\begin{aligned}
|0_{c_1}H_{k_1}H_{k_2}\rangle &\rightarrow \big(-\gamma|H\rangle_{f_1} + \sqrt{1-\gamma^2}|H\rangle_{e_1}\big)\otimes\big(-|H\rangle_{f_2}\big)\\
&= \gamma|H\rangle_{f_1}|H\rangle_{f_2} - \sqrt{1-\gamma^2}|H\rangle_{e_1}|H\rangle_{f_2}. \qquad (12)
\end{aligned}$$

If both the spatial modes f_1 and f_2 contain one photon, $|0_{c_1}H_{k_1}H_{k_2}\rangle$ will collapse to $\frac{\gamma}{2}|0_{\text{out}}\rangle(|H_{D_1}H_{D_3}\rangle + |H_{D_1}V_{D_4}\rangle + |V_{D_2}H_{D_3}\rangle + |V_{D_2}V_{D_4}\rangle)$, after passing through QWP1 and QWP2. QWP is the quarter-wave plate which acts as the role of the Hadamard operation. In order to ensure that the spatial modes f_1 and f_2 both contain one photon, this protocol requires the single-photon detectors to distinguish the photon number in the output modes. If the spatial mode f_1 or f_2 contains two photons, this protocol fails.

The mixed state ρ'_{θ_j} combined with the polarization Bell state $|\phi_1\rangle$ can be described as follows. With the probability of F, it is in the state $|\varphi\rangle\otimes|\phi_1\rangle$ and with the probability of $1-F$, it is in the state $|\text{vac}\rangle\otimes|\phi_1\rangle$. We first discuss the item $|\varphi\rangle\otimes|\phi_1\rangle$. It evolves as

$$\begin{aligned}
|\varphi\rangle\otimes|\phi_1\rangle = \Big(&\frac{\alpha}{\sqrt{2}}\big|+_{\theta_j}\big\rangle_{c_1}|0\rangle_{d_1}|0\rangle_{m_1}|0\rangle_{n_1}\\
&+ \frac{\beta}{\sqrt{2}}|0\rangle_{c_1}\big|+_{\theta_j}\big\rangle_{d_1}|0\rangle_{m_1}|0\rangle_{n_1}\\
&+ \frac{\tau}{\sqrt{2}}|0\rangle_{c_1}|0\rangle_{d_1}\big|+_{\theta_j}\big\rangle_{m_1}|0\rangle_{n_1}\\
&+ \frac{\delta}{\sqrt{2}}|0\rangle_{c_1}|0\rangle_{d_1}|0\rangle_{m_1}\big|+_{\theta_j}\big\rangle_{n_1}\Big)\\
&\otimes\frac{1}{\sqrt{2}}(|H\rangle_{k_1}|H\rangle_{k_2} + |V\rangle_{k_1}|V\rangle_{k_2}). \qquad (13)
\end{aligned}$$

The first item evolves as

$$\begin{aligned}
&\frac{\alpha}{\sqrt{2}}\big|+_{\theta_j}\big\rangle_{c_1}|0\rangle_{d_1}|0\rangle_{m_1}|0\rangle_{n_1}\\
&\otimes\frac{1}{\sqrt{2}}(|H\rangle_{k_1}|H\rangle_{k_2} + |V\rangle_{k_1}|V\rangle_{k_2})\\
&= \frac{\alpha}{2\sqrt{2}}(|H\rangle_{c_1}|H\rangle_{k_1}|H\rangle_{k_2} + |H\rangle_{c_1}|V\rangle_{k_1}|V\rangle_{k_2}\\
&\quad + e^{i\theta}|V\rangle_{c_1}|H\rangle_{k_1}|H\rangle_{k_2} + e^{i\theta}|V\rangle_{c_1}|V\rangle_{k_1}|V\rangle_{k_2})\\
&\otimes|0\rangle_{d_1}|0\rangle_{m_1}|0\rangle_{n_1}\\
&\rightarrow \frac{\alpha}{2\sqrt{2}}\Big[\frac{(2\gamma^2-1)}{2}|H_{\text{out}}\rangle\big(|H_{D_1}H_{D_3}\rangle + |H_{D_1}V_{D_4}\rangle\\
&\quad + |V_{D_2}H_{D_3}\rangle + |V_{D2}V_{D4}\rangle\big)|0\rangle_{d_1}|0\rangle_{m_1}|0\rangle_{n_1}\\
&\quad + \frac{\gamma^2}{2}|H_{\text{out}}\rangle\big(|H_{D_1}H_{D_3}\rangle - |H_{D_1}V_{D_4}\rangle\\
&\quad - |V_{D_2}H_{D_3}\rangle + |V_{D_2}V_{D_4}\rangle\big)|0\rangle_{d_1}|0\rangle_{m_1}|0\rangle_{n_1}\\
&\quad + e^{i\theta}\frac{\gamma^2}{2}|V_{\text{out}}\rangle\big(|H_{D_1}H_{D_3}\rangle + |H_{D_1}V_{D_4}\rangle\\
&\quad + |V_{D_2}H_{D_3}\rangle + |V_{D_2}V_{D_4}\rangle\big)|0\rangle_{d_1}|0\rangle_{m_1}|0\rangle_{n_1}\\
&\quad + e^{i\theta}\frac{(2\gamma^2-1)}{2}|V_{\text{out}}\rangle\big(|H_{D_1}H_{D_3}\rangle - |H_{D_1}V_{D_4}\rangle\\
&\quad - |V_{D_2}H_{D_3}\rangle + |V_{D_2}V_{D_4}\rangle\big)|0\rangle_{d_1}|0\rangle_{m_1}|0\rangle_{n_1}\Big]. \qquad (14)
\end{aligned}$$

The second item evolves as

$$\begin{aligned}
&\frac{\beta}{\sqrt{2}}|0\rangle_{c_1}\big|+_{\theta_j}\big\rangle_{d_1}|0\rangle_{m_1}|0\rangle_{n_1}\\
&\otimes\frac{1}{\sqrt{2}}\big(|H\rangle_{k_1}|H\rangle_{k_2} + |V\rangle_{k_1}|V\rangle_{k_2}\big)\\
&\rightarrow \frac{\beta\gamma}{4}\big[|0_{\text{out}}\rangle\big(|H_{D_1}H_{D_3}\rangle + |H_{D_1}V_{D_4}\rangle\\
&\quad + |V_{D_2}H_{D_3}\rangle + |V_{D_2}V_{D_4}\rangle\big)\\
&\quad + |0_{\text{out}}\rangle\big(|H_{D_1}H_{D_3}\rangle - |H_{D_1}V_{D_4}\rangle - |V_{D_2}H_{D_3}\rangle\\
&\quad + |V_{D_2}V_{D_4}\rangle\big)\big]\otimes\big|+_{\theta_j}\big\rangle_{d_1}|0\rangle_{m_1}|0\rangle_{n_1}\\
&= \frac{\beta\gamma}{4}|0_{\text{out}}\rangle\big|+_{\theta_j}\big\rangle_{d_1}|0\rangle_{m_1}|0\rangle_{n_1}\big(|H_{D_1}H_{D_3}\rangle + |V_{D_2}V_{D_4}\rangle\big). \qquad (15)
\end{aligned}$$

The third item evolves as

$$\begin{aligned}&\frac{\tau}{\sqrt{2}}|0\rangle_{c_1}|0\rangle_{d_1}|+_{\theta_j}\rangle_{m_1}|0\rangle_{n_1}\\&\otimes\frac{1}{\sqrt{2}}\left(|H\rangle_{k_1}|H\rangle_{k_2}+|V\rangle_{k_1}|V\rangle_{k_2}\right)\\&\rightarrow\ \frac{\tau\gamma}{4}|0_{\text{out}}\rangle|0\rangle_{d_1}|+_{\theta_j}\rangle_{m_1}|0\rangle_{n_1}\left(|H_{D_1}H_{D_3}\rangle+|V_{D_2}V_{D_4}\rangle\right).\end{aligned}\tag{16}$$

The fourth item evolves as

$$\begin{aligned}&\frac{\delta}{\sqrt{2}}|0\rangle_{c_1}|0\rangle_{d_1}|0\rangle_{m_1}|+_{\theta_j}\rangle_{n_1}\\&\otimes\frac{1}{\sqrt{2}}\left(|H\rangle_{k_1}|H\rangle_{k_2}+|V\rangle_{k_1}|V\rangle_{k_2}\right)\\&\rightarrow\ \frac{\delta\gamma}{4}|0_{\text{out}}\rangle|0\rangle_{d_1}|0\rangle_{m_1}|+_{\theta_j}\rangle_{n_1}\left(|H_{D_1}H_{D_3}\rangle+|V_{D_2}V_{D_4}\rangle\right).\end{aligned}\tag{17}$$

The item $|0\rangle\otimes|\phi_1\rangle$ evolves as

$$\begin{aligned}|0\rangle\otimes|\phi_1\rangle\ &=\ |0\rangle\otimes\frac{1}{\sqrt{2}}\left(|H\rangle_{k_1}|H\rangle_{k_2}+|V\rangle_{k_1}|V\rangle_{k_2}\right)\\&\rightarrow\frac{\gamma}{\sqrt{2}}|0\rangle\left(|H_{D_1}H_{D_3}\rangle+|V_{D_2}V_{D_4}\rangle\right).\end{aligned}\tag{18}$$

Interestingly, from Eqs. (14) to (18), if they pick up the case that the single-photon detectors D_1D_4 or D_2D_3 each register one photon, they will obtain the state $|+_{\theta_j}\rangle$ deterministically in the output mode, for the cases in Eqs. (15) to (18) cannot lead to both single-photon detectors D_1D_4 or D_2D_3 registering one photon, and only the items in Eq. (14) can satisfy the selection condition.

Once Bob obtains the single-photon state $|+_{\theta_j}\rangle$ deterministically, he can start to perform the BQC protocol. In this way, the whole BQC protocol can be modified as follows: (1) Alice prepares n rotated qubits $\{|+_{\theta_j}\rangle\}_{j=1}^{n}$. (2) Alice encodes the photon $|+_{\theta_j}\rangle$ with linear optics as shown in Fig. 2. (3) Alice distributes the photon to Bob, which will suffer from collective noise and photon loss. (4) Bob distills the polluted single-photon states with the noise processer as shown in Fig. 3. If it is a failure, Bob asks Alice to resend the single photon and repeat steps (1)–(4). (5) Bob prepares the graph state G. (6) Bob performs the measurement on the jth qubit. (7) Bob sends the measurement results to Alice, and Alice completes the computation with a classical computer.

III. DISCUSSION

So far, we have completely explained the antinoise single-sever BQC protocol. In the original BQC protocol, Alice prepares and distributes the state $|+_{\theta_j}\rangle$ directly. Bob also receives the $|+_{\theta_j}\rangle$ and performs the BQC subsequently, for they do not consider the noise environment. Similarly to the pioneer work of Ref. [25] on the collective-noise BQC protocol, Alice and Bob should perform the pretreatment for noise, before starting the BQC protocol, following the approaches suggested in Refs. [28,35]. In the BQC protocol, two essential properties are correctness and blindness. Correctness means that the output of the protocol is Alice's desired one as long as Alice and Bob follow the procedure of the protocol faithfully. The blindness means that Bob cannot know any information about Alice's inputs, algorithm, and outputs. Obviously, this protocol is correct as Bob can obtain the faithful qubits after the noise processer. Meanwhile, this protocol is blind. The information from Alice to Bob is $|+_{\theta_j}\rangle$, which is decided by θ_j. Bob does not know the exact information of θ_j, which ensures that the protocol is blind.

We can calculate the total success probability of this protocol. From Fig. 2, we explain this protocol by selecting the case that the photon is in the spatial mode a_1 with the probability of 50%. Actually, if the photon is in the spatial mode b_1, we can perform the protocol in the same principle. That is to say, if the photon is not lost and only suffers from the collective noise, by picking up the suitable arriving time SL (LS) as shown in Fig. 4, the total success probability is 50%. On the other hand, as shown in Fig. 3, such setup essentially distills the photon in the spatial modes c_1, i.e., the first item in Eq. (7). Actually, in Eq. (7), three other items which contain the single photon can also be verified by adding three auxiliary polarized Bell states. The final success probability of this protocol can be calculated as

$$P=\frac{F(\gamma^2-1)^2}{16}.\tag{19}$$

From Eq. (19), if $\gamma=0$, we can obtain the maximal success probability. Actually, $\gamma=0$ means that the PPBS becomes the PBS. The previous work [25] presented three important BQC protocols over a collective-noise channel. The first protocol is the entanglement-based protocol with the success probability T^2. T is the transmission efficiency, similar to F in this protocol. The second is the single-photon-based protocol with the success probability $O(T^2)$. If $T\ll 1$, the success probabilities T^2 and $O(T^2)$ will become low. The third is the coherent-light-assisted protocol and the success probability is improved to $O(T)$. From Fig. 6 in Ref. [25], the success probability can be increased up to $\frac{T}{2}$ by increasing the mean photon number of the ancillary coherent light to be infinite. From Eq. (19), the success probability in our protocol can be increased to $\frac{F}{16}$, which is smaller than that of the coherent-light-assisted protocol. One the other hand, Ref. [25] considers the collective noise and the photon loss. More precisely, the photon loss is introduced as the transmittance T. In their protocols, Bob can perform perfect quantum nondemolition (QND) measurement, which can distinguish the number of arriving photons deterministically without destroying them. In principle, QND measurements can be done with unit probability. For example, QND measurement implemented with cross-Kerr nonlinearity can reach unit probability in theory, which has been widely discussed in quantum information processing protocols [36–40]. In our protocol, with linear optics, we provide an alternative approach to deal with the photon loss and realize the QND measurement probabilistically. All three protocols require auxiliary resources, such as entanglement, single photons, or coherent light, which make their protocols more sophisticated.

IV. CONCLUSION

In conclusion, we have described an efficient antinoise single-server BQC protocol. This protocol has several advantages. First, the client Alice does not require any auxiliary resources, which makes the client economic. Second, this

protocol not only can protect the quantum state from the collective noise, but also from the photon loss. Third, the noise processer for Bob is based on the linear optics so that it is feasible in experiment. This protocol combined with the previous BQC protocols over a collective-noise channel may have the potential applications in future BQC under a noisy environment.

ACKNOWLEDGMENTS

This work was supported by the National Natural Science Foundation of China under Grant No. 11474168 and the China Postdoctoral Science Foundation under Grant No. 2018M642293.

[1] P. W. Shor, in *Proceedings of the 35th Annual Symposium on Foundations of Computer Science* (IEEE, New York, 1994), p. 124.

[2] L. K. Grover, in *Proceedings of the Twenty-Eighth Annual ACM Symposium on Theory of Computing* (ACM Press, New York,1996), p. 212.

[3] G. L. Long, Phys. Rev. A **64**, 022307 (2001).

[4] J. I. Cirac and P. Zoller, Phys. Rev. Lett. **74**, 4091 (1995).

[5] Y. Makhlin, G. Schön, and A. Shnirman, Rev. Mod. Phys. **73**, 357 (2001).

[6] J. Berezovsky, M. H. Mikkelsen, N. G. Stoltz, L. A. Coldren, and D. D. Awschalom, Science **320**, 349 (2008); R. Hanson and D. D. Awschalom, Nature (London) **453**, 1043 (2008).

[7] A. M. Childs, Quantum Inf. Comput. **5**, 456 (2005).

[8] A. Broadbent, J. Fitzsimons, and E. Kashefi, in *Proceedings of the 50th Annual IEEE Symposium on Foundations of Computer Science* (IEEE, Piscataway, NJ, 2009), p. 517.

[9] T. Morimae, V. Dunjko, and E. Kashefi, Quantum Inf. Comput. **15**, 200 (2015).

[10] T. Morimae and K. Fujii, Nat. Commun. **3**, 1036 (2012).

[11] J. F. Fitzsimons and E. Kashefi, Phys. Rev. A **96**, 012303 (2017).

[12] T. Morimae, Phys. Rev. Lett. **109**, 230502 (2012).

[13] V. Dunjko, E. Kashefi, and A. Leverrier, Phys. Rev. Lett. **108**, 200502 (2012).

[14] T. Morimae and K. Fujii, Phys. Rev. A **87**, 050301(R) (2013).

[15] T. Sueki, T. Koshiba, and T. Morimae, Phys. Rev. A **87**, 060301(R) (2013).

[16] S. Barz, E. Kashefi, A. Broadbent, J. F. Fitzsimons, A. Zeilinger, and P. Walther, Science **335**, 303 (2012).

[17] T. Morimae and K. Fujii, Phys. Rev. Lett. **111**, 020502 (2013).

[18] V. Giovannetti, L. Maccone, T. Morimae, and T. G. Rudolph, Phys. Rev. Lett. **111**, 230501 (2013).

[19] A. Mantri, C. A. Perez-Delgado, and J. F. Fitzsimons, Phys. Rev. Lett. **111**, 230502 (2013).

[20] K. A. G. Fisher, A. Broadbent, L. K. Shalm, Z. Yan, J. Lavoie, R. Prevedel, T. Jennewein, and K. J. Resch, Nat. Commun. **5**, 3074 (2014).

[21] T. Morimae, Phys. Rev. A **89**, 060302(R) (2014).

[22] A. Gheorghiu, E. Kashefi, and P. Wallden, New J. Phys. **17**, 083040 (2015).

[23] Q. Li, W. H. Chan, C. Wu, and Z. Wen, Phys. Rev. A **89**, 040302(R) (2014).

[24] Y. B. Sheng and L. Zhou, Sci. Rep. **5**, 7815 (2015).

[25] Y. Takeuchi, K. Fujii, R. Ikuta, T. Yamamoto, and N. Imoto, Phys. Rev. A **93**, 052307 (2016).

[26] J. F. Fitzsimons, npj Quantum Inf. **3**, 23 (2017).

[27] K. Xu and H.-K. Lo, arXiv:1508.07910.

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

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

[30] D. Kalamidas, Phys. Lett. A **343**, 331 (2005).

[31] T. Yamamoto, J. Shimamura, S. K. Özdemir, M. Koashi, and N. Imoto, Phys. Rev. Lett. **95**, 040503 (2005).

[32] T. Yamamoto, K. Hayashi, Ş. K. Özdemir, M. Koashi, and N. Imoto, Nat. Photon. **2**, 488 (2008).

[33] Y. B. Sheng and F. G. Deng, Phys. Rev. A **81**, 042332 (2010).

[34] H. Kumagai, T. Yamamoto, M. Koashi, and N. Imoto, Phys. Rev. A **87**, 052325 (2013).

[35] E. Meyer-Scott, M. Bula, K. Bartkiewicz, A. Černoch, J. Soubusta, T. Jennewein, and K. Lemr, Phys. Rev. A **88**, 012327 (2013).

[36] K. Nemoto and W. J. Munro, Phys. Rev. Lett. **93**, 250502 (2004).

[37] B. He, Y. Ren, and J. A. Bergou, Phys. Rev. A **79**, 052323 (2009).

[38] Y. B. Sheng, L. Zhou, S. M. Zhao, and B. Y. Zheng, Phys. Rev. A **85**, 012307 (2012).

[39] L. Dong, J. X. Wang, Q. Y. Li, H. Z. Shen, H. K. Dong, X. M. Xiu, Y. J. Gao, and C. H. Oh, Phys. Rev. A **93**, 012308 (2016).

[40] P. Kok, W. J. Munro, K. Nemoto, T. C. Palph, J. P. Dowling, and G. J. Milburn, Rev. Mod. Phys. **79**, 135 (2007).