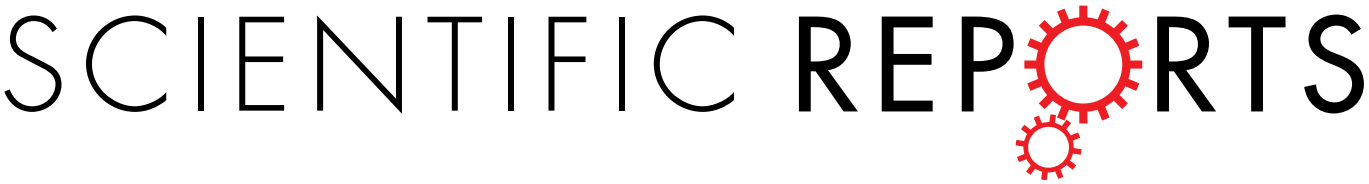

OPEN

Greenberger-Horne-Zeilinger states-based blind quantum computation with entanglement concentration

Received: 24 March 2017
Accepted: 16 June 2017
Published online: 11 September 2017

Xiaoqian Zhang[1], Jian Weng[1], Wei Lu[2], Xiaochun Li[3], Weiqi Luo[1] & Xiaoqing Tan[3]

In blind quantum computation (BQC) protocol, the quantum computability of servers are complicated and powerful, while the clients are not. It is still a challenge for clients to delegate quantum computation to servers and keep the clients' inputs, outputs and algorithms private. Unfortunately, quantum channel noise is unavoidable in the practical transmission. In this paper, a novel BQC protocol based on maximally entangled Greenberger-Horne-Zeilinger (GHZ) states is proposed which doesn't need a trusted center. The protocol includes a client and two servers, where the client only needs to own quantum channels with two servers who have full-advantage quantum computers. Two servers perform entanglement concentration used to remove the noise, where the success probability can almost reach 100% in theory. But they learn nothing in the process of concentration because of the no-signaling principle, so this BQC protocol is secure and feasible.

Blind quantum computation (i.e. BQC)[1–7] is still a challenging research field, where a client has not enough quantum computability, and delegates her quantum computing to the servers who have full-advanced quantum computers. In long-distance BQC, quantum entanglement plays an important role and three mainly blind entangled states have already been studied which are blind brickwork state[1], blind topological state[2] and Affleck-Kennedy-LiebTasaki (i.e. AKLT) state[3]. Some BQC protocols[1,4–6] are based on the blind brickwork state which is proposed by Broadbent *et al.*[1]. Later, Barz *et al.*[7] demonstrated the blindness of the brickwork state. Broadbent *et al.*[1] in 2009 proposed a single-server BQC protocol based on single-qubit states and double-server BQC protocol based on the entanglement swapping of Bell states. However, the quantum entanglement of Bell states in double-server BQC protocol[1] will suffer quantum channel loss due to the influence of noisy channel. To solve this problem, Morimae and Fujii[4] proposed a method of entanglement distillation to extract high-fidelity Bell states, meanwhile its security can also be guaranteed. Li *et al.*[5] proposed a triple-server BQC protocol based on Bell states. Sheng and Zhou[6] proposed a double-server BQC protocol based on Bell states, where the deterministic entanglement distillation can remove the noise that transforms pure entangled states into mixed entangled states. As we can see that the aims of BQC protocols[1,4–6] are all to obtain the single-qubit states $\left|\pm_{\theta_i}\right\rangle$ with $\theta_i \in \left\{0, \frac{\pi}{4}, \frac{2\pi}{4}, \ldots, \frac{7\pi}{4}\right\}$ to create the blind brickwork states[1]. The other two blind graph states[2,3] can also be used to perform BQC successfully. The Raussendorf-Harrington-Goyal (i.e. RHG) lattice[2], which the blindness is guaranteed in a topological manner, is used to perform four quantum measurements $\{X, Y, Z, T\}$ only known by clients. Compared with the cluster states, AKLT states can be prepared efficiently and simply in linear optics with biphotons[8]. Recently, more and more interesting BQC protocols are proposed[9–18]. In BQC, the quantum channel noise is still an urgent problem. Previous works[4,6,14] have studied quantum channel noises in BQC protocols. For example, Takeuchi *et al.*[14] proposed three BQC protocols based on decoherence-free subspace (i.e. DFS) to resist the collective noise of quantum channel.

The new BQC protocol is based on maximally GHZ entangled states, where there are three participants (a client Alice, two servers Bob and Charlie). The BQC protocol is divided into four steps. First, Bob prepares initial GHZ states, remains one photon and sends other two photons to Alice. Alice disturbs the orders of two photons and sends to Charlie. Second, Bob and Charlie perform entanglement concentration to get ideal maximally entangled states, where two identical less-entangled states can be used to concentrate a maximally entangled state by two-step

[1]Department of Computer Science, Jinan University, Guangzhou, 510632, China. [2]School of Data and Computer Science, SunYat-sen University, Guangzhou, 510006, China. [3]Department of Mathematics, Jinan University, Guangzhou, 510632, China. Correspondence and requests for materials should be addressed to J.W. (email: cryptjweng@gmail.com)

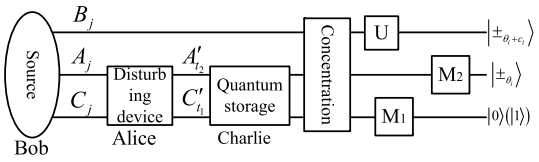

Figure 1. Schematic diagram of BQC protocol is based on maximally GHZ entangled states with z-basis ($\{|0\rangle, |1\rangle\}$) measurement M_1, basis $|0\rangle \pm e^{-i\theta_j}|1\rangle$ measurement M_2, Pauli operations U, Bell measurement BM, Charlie's measurement outcome c_i. The order of photons sequences A_j and C_j ($j \in \{1, 2, 3, \ldots, n\}$) are disturbed and rewritten as A'_{t_2} and C'_{t_1} ($t_1, t_2 \in \{1, 2, 3, \ldots, n\}$). Photons A'_{t_2} and C'_{t_1} belong to Charlie, and B_j belongs to Bob, where A'_{t_2}, B_j and C'_{t_1} ($t_1 \neq t_2 \neq j$) belong to a GHZ state.

parity check and project measurements. Third, Bob performs Pauli operations on his photons under Alice's instruction. Then Charlie performs measurement on one photon with the basis $\{|0\rangle, |1\rangle\}$. Alice randomly chooses $\theta_i\left(\in\left\{0,\frac{\pi}{4}, \ldots, \frac{7\pi}{4}\right\}\right)$ and sends to Charlie. Charlie performs measurement on the other photon and Bob gets the single-qubit. Finally, Alice and Bob perform single-server BQC protocol.

This BQC protocol has four contributions. First, two servers can communication with each other without degrading the security. Second, it does not need a trusted center. The task of preparing initial entangled states can be assigned to Bob. Third, Bob and Charlie don't need to exchange their classical information. If they collude, they don't know any information about Alice's inputs, outputs and algorithms. The last one, entanglement concentration can be used to remove the channel noise.

Results

BQC protocol based on maximally GHZ entangled states. Photons are the best physical systems for the long-distance transmission of entangled states, thus entangled photons states are used as quantum information carriers in BQC. In this BQC protocol, we use $|0\rangle$ and $|1\rangle$ to express photons. In entanglement concentration, we use $|H\rangle$ and $|V\rangle$ to express photons, where $|H\rangle$ is equal to $|0\rangle$ and $|V\rangle$ is equal to $|1\rangle$. In this section, we propose the BQC protocol based on maximally GHZ photons entangled states $|GHZ\rangle_{A_jB_jC_j} = \frac{1}{2}(|001\rangle + |010\rangle + |100\rangle + |111\rangle)$ ($j = 1, 2, \ldots, n$) (Fig. 1). The cross-Kerr nonlinear can be used to construct a CNOT gate in ref. 19. There are also many other methods to realize it[19–23]. In the BQC protocol, we suppose that these quantum devices are all ideal. The client owns quantum channels with two servers and quantum disturbing device.

- Bob generates enough maximally GHZ entangled states $|GHZ\rangle_{A_jB_jC_j}$, where the subscripts A_j, B_j and C_j represents photons A_j, B_j and C_j. Bob keeps photons sequences $S_B = [B_1, B_2, \ldots, B_n]$ and sends photons sequences $S_A = [A_1, A_2, \ldots, A_n]$ and $S_C = [C_1, C_2, \ldots, C_n]$ to Alice successively. After receiving photons sequences, Alice disturbs the order of photons sequences S_A and S_C. The reordered photons sequences are rewritten as $S_{A'} = [A'_1, A'_2, \ldots, A'_n]$ and $S_{C'} = [C'_1, C'_2, \ldots, C'_n]$, meanwhile $|GHZ\rangle_{A_jB_jC_j}$ is remarked as $|GHZ\rangle_{A'_{t_2}B_jC'_{t_1}}$ ($t_1, t_2 \in \{1, 2, \cdots, n\}$). The orders of photons sequences $S_{A'}$ and $S_{C'}$ are different and only known by Alice. Then Alice sends photons sequences $S_{A'}$ and $S_{C'}$ to Charlie. Due to the effect of quantum channel noise, the maximally entangled states $|GHZ\rangle_{A'_{t_2}B_jC'_{t_1}}$ evolve into less-entangled states $|GHZ'\rangle_{A'_{t_2}B_jC'_{t_1}} = \alpha|001\rangle + \beta|010\rangle + \delta|100\rangle + \eta|111\rangle$, where $|\alpha|^2 + |\beta|^2 + |\delta|^2 + |\eta|^2 = 1$. In order to get states $|GHZ\rangle_{A'_{t_2}B_jC'_{t_1}}$, Bob and Charlie firstly perform entanglement concentration.
- Bob performs one of four operations $\{I, \sigma_x, i\sigma_y, \sigma_z\}$ randomly chosen by Alice on photons B_j and $|GHZ\rangle_{A'_{t_2}B_jC'_{t_1}}$ states evolve into one of four states $\left\{|GHZ_1\rangle_{A'_{t_2}B_jC'_{t_1}}, |GHZ_2\rangle_{A'_{t_2}B_jC'_{t_1}}, |GHZ_3\rangle_{A'_{t_2}B_jC'_{t_1}}, |GHZ_4\rangle_{A'_{t_2}B_jC'_{t_1}}\right\}$.

$$
\begin{aligned}
\xrightarrow{I}|GHZ_1\rangle_{A'_{t_2}B_jC'_{t_1}} &= \frac{1}{2}(|001\rangle + |010\rangle + |100\rangle + |111\rangle)\\
&= \frac{1}{2\sqrt{2}}(|\psi^+\rangle_{A'_{t_2}B_j}|0\rangle_{C'_{t_1}} + |\phi^+\rangle_{A'_{t_2}B_j}|1\rangle_{C'_{t_1}}),\\
\xrightarrow{\sigma_x}|GHZ_2\rangle_{A'_{t_2}B_jC'_{t_1}} &= \frac{1}{2}(|011\rangle + |000\rangle + |110\rangle + |101\rangle)\\
&= \frac{1}{2\sqrt{2}}(|\phi^+\rangle_{A'_{t_2}B_j}|0\rangle_{C'_{t_1}} + |\psi^+\rangle_{A'_{t_2}B_j}|1\rangle_{C'_{t_1}}),\\
\xrightarrow{i\sigma_y}|GHZ_3\rangle_{A'_{t_2}B_jC'_{t_1}} &= \frac{1}{2}(-|011\rangle + |000\rangle - |110\rangle + |101\rangle)\\
&= \frac{1}{2\sqrt{2}}(|\phi^-\rangle_{A'_{t_2}B_j}|0\rangle_{C'_{t_1}} - |\psi^-\rangle_{A'_{t_2}B_j}|1\rangle_{C'_{t_1}}),\\
\xrightarrow{\sigma_z}|GHZ_4\rangle_{A'_{t_2}B_jC'_{t_1}} &= \frac{1}{2}(|001\rangle - |010\rangle + |100\rangle - |111\rangle)\\
&= \frac{1}{2\sqrt{2}}(-|\psi^-\rangle_{A'_{t_2}B_j}|0\rangle_{C'_{t_1}} + |\phi^-\rangle_{A'_{t_2}B_j}|1\rangle_{C'_{t_1}}).
\end{aligned}
\tag{1}
$$

Since the orders of sequences $S_{A'}$, S_B and $S_{C'}$ are different, both Bob and Charlie cannot know which state $|GHZ_u\rangle_{A'_{t_2}B_jC'_{t_1}}$ ($u\in\{1, 2, 3, 4\}$) they shared.

- Charlie performs measurement on photons C'_{t_1} using the basis $\{|0\rangle, |1\rangle\}$ under the guidance of Alice. Alice randomly chooses $\theta_i \in \{0, \pi/4, 2\pi/4, \ldots, 7\pi/4\}$ and sends to Charlie. Charlie performs measurement on the basis $\{|0\rangle \pm e^{-i\theta_i}|1\rangle\}$ and Bob obtains photons states $|\pm_{\theta_i+c_i\pi}\rangle$, where c_i ($\in\{0, 1\}$) is Charlie's measurement outcome. Because the orders of A'_{t_2} and B_j are different, Bob can not know anything even if Charlie tells the value of θ_i to Bob.
- Alice, Bob and Charlie repeat (1–3) steps such that Bob obtains single-photon states $\bigotimes_{i=1}^{n}|\pm_{\theta_i+c_i\pi}\rangle$ successfully.

  The remaining steps are the same as steps (2–3) of the BFK protocol[1] or steps (2–5) of blind topological BQC protocol[2]. The blindness of graph states and the correctness of quantum computation have already been exhibited in refs 1 and 2 in detail.

In the step 1 of this BQC, entanglement concentration is used to remove the noise. In the following, the process of entanglement concentration is showed with optical system.

Entanglement concentration of pure maximally GHZ entangled state. In a practical transmission, there exist two kinds of quantum channel noises, i.e. pure maximally entangled states evolve into mixed states or less-entangled states. Entanglement purification[24–28] is applied to extract high-fidelity maximally entangled states from mixed entangled states. Entanglement concentration[29–45] is often used to distill less-entangled states into pure maximally entangled states by local operations and classical communication (i.e. LOCC). Bennett *et al.*[29] firstly proposed an entanglement concentration protocol by using Schmidt projection. In 2003, Zhao *et al.*[42] not only demonstrated the entanglement concentration scheme in ref. 30 but also verified a quantum repeater in experiment. Li *et al.*[39] proposed two protocols to concentrate hyper-entangled GHZ states by using a single-photon state of two freedoms and two less-entangled states respectively. Sheng *et al.*[32] proposed to concentrate arbitrary W states by using two steps. Afterwards, a universal concentration scheme of an arbitrary less-entangled N-photon W state is proposed in ref. 43. Here, we consider a special quantum channel noise, i.e. pure maximally entangled states evolve into less-entangled states, which can be distilled by entanglement concentration. In the following, we give the entanglement concentration of GHZ states that were experimentally prepared in refs 46–48.

The first round of entanglement concentration. In the BQC, the maximally GHZ states can be rewritten in the form of

$$|GHZ\rangle_{a_1b_1c_1} = \frac{1}{2}(|HHV\rangle + |HVH\rangle + |VHH\rangle + |VVV\rangle), \tag{2}$$

where we define $|H\rangle = |0\rangle$ and $|V\rangle = |1\rangle$. The subscripts a_1, b_1 and c_1 represent the spatial-mode of photons A'_{t_2}, B_j and C'_{t_1}. We consider the noisy model that pure maximally entangled states evolve pure less entangled states. Suppose less-entangled pure photons states are

$$|GHZ'\rangle_{a_1b_1c_1} = \alpha|HHV\rangle + \beta|HVH\rangle + \delta|VHH\rangle + \eta|VVV\rangle, \tag{3}$$

where four real numbers $\alpha, \beta, \delta, \eta$ satisfy $|\alpha|^2+|\beta|^2+|\delta|^2+|\eta|^2=1$.

Two identical less-entangled states, which the parameters are all unknown, can distill a maximally entangled state in Eq. (2). The schematic of entanglement concentration is shown in Fig. 2. Here, only Alice knows whether entanglement concentration is successful and the correct orders of A'_{t_2}, B_j and C'_{t_1}.

After passing $HWP_{90°}$, the state $|GHZ'\rangle_{a_1b_1c_1}$ evolves to

$$|GHZ'\rangle_{a_2b_2c_2} = \alpha|VVH\rangle + \beta|VHV\rangle + \delta|HVV\rangle + \eta|HHH\rangle, \tag{4}$$

where polarization photons a_1, b_1 and c_1 are flipped and relabeled as a_2, b_2 and c_2.

The entanglement concentration is divided into two steps. In the first step, the system composed of six photons is

$$\begin{aligned}
|\Psi\rangle_{a_1b_1c_1a_2b_2c_2} &= |GHZ'\rangle_{a_1b_1c_1} \otimes |GHZ'\rangle_{a_2b_2c_2} \\
&= [\alpha^2|HHVVVH\rangle + \beta^2|HVHVHV\rangle \\
&\quad +\delta^2|VHHHVV\rangle + \eta^2|VVVHHH\rangle] \\
&\quad +[\alpha\beta(|HHVVHV\rangle + |HVHVVH\rangle) \\
&\quad +\delta\eta(|HHVHVV\rangle + |VHHVVH\rangle)] \\
&\quad +[\alpha\delta(|HVHHHH\rangle + |VVVVHV\rangle) \\
&\quad +\beta\eta(|VHHHHH\rangle + |VVVHVV\rangle)] \\
&\quad +[\alpha\eta|HHVHHH\rangle + |VVVVVH\rangle \\
&\quad +\beta\delta(|HVHHVV\rangle + |VHHVHV\rangle)]
\end{aligned} \tag{5}$$

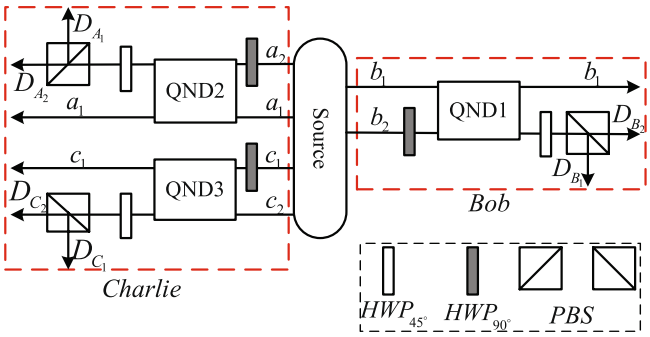

Figure 2. The schematic diagram of polarization-entanglement concentration. The sources is used to produce polarization-entangled states. Photons $a_1(a_2)$ and $c_1(c_2)$ belong to Charlie, where Bob retains photons $b_1(b_2)$. HWP is half-wave plate which HWP_{90° flips the horizontal and vertical polarization states. HWP_{45° just likes a Hadamard operation to rotate horizontal and vertical polarization states. The polarizing beam splitters (PBSs) are used to transmit horizontal polarization $|H\rangle$ and reflect vertical polarization $|V\rangle$. QND_i (with $i = 1, 2, 3$) represents quantum nondemolition detections. Detectors D_{B_1} and D_{B_2} belong to Bob, D_{A_1}, D_{A_2}, D_{C_1} and D_{C_2} belong to Charlie.

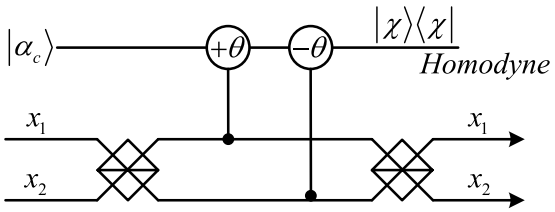

Figure 3. Schematic diagram of QND[49]. $\pm\theta = \chi t$ represents the cross-Kerr nonlinearity media that introduces the phase shift θ when photons pass through the media. $|\chi\rangle\langle\chi|$ is homodyne measurement that can distinguish different phase shifts. The signal photons $|\alpha_1\rangle$, $|\alpha_2\rangle$ and $|\alpha_3\rangle$ are related to a_1 and a_2, b_1 and b_2, c_1 and c_2 respectively. Here x_1 and x_2 can be specifically expressed as a_1 and a_2 (b_1 and b_2, c_1 and c_2).

After both a_1 and a_2 (b_1 and b_2, c_1 and c_2) pass parity check device (Fig. 3), Bob and Charlie can get some specific quantum state by choosing phase shifts. Here, we suppose that Bob and Charlie are honest to perform the entanglement concentration. The concrete process of the parity check device is given in Methods.

For b_1 and b_2, a_1 and a_2, c_1 and c_2, if Bob and Charlie all choose $\pm 2\theta$ phase shifts of odd-parity check states, the state is

$$\begin{aligned} |\varphi_1\rangle_{a_1b_1c_1a_2b_2c_2} &= \alpha^2|HHV\rangle|VVH\rangle + \beta^2|HVH\rangle|VHV\rangle \\ &\quad +\delta^2|VHH\rangle|HVV\rangle + \eta^2|VVV\rangle|HHH\rangle \end{aligned} \tag{6}$$

with the probability $p_{11}^1 = \alpha^4 + \beta^4 + \delta^4 + \eta^4$, where p_{vj}^m represents the probability of obtaining $|\varphi_1\rangle_{a_1b_1c_1a_2b_2c_2}$ with the number of rounds $v(v = 1, 2, 3, \ldots, k)$, the number of steps j ($j = 1, 2$) in vth round and the quantum state m ($m = 1, 2, 3, 4$) in jth step of vth round.

If Bob chooses 0 phase shift of even-parity check states for b_1 and b_2, Charlie chooses 0 phase shift of even-parity check states for c_1 and c_2, and $\pm 2\theta$ phase shift of odd-parity check states for a_1 and a_2, the state is

$$\begin{aligned} |\varphi_2\rangle_{a_1b_1c_1a_2b_2c_2} &= \alpha\beta(|HHV\rangle|VHV\rangle + |HVH\rangle|VVH\rangle) \\ &\quad +\delta\eta(|VHH\rangle|HHH\rangle + |VVV\rangle|HVV\rangle) \end{aligned} \tag{7}$$

with the probability $p_{11}^2 = 2(\alpha^2\beta^2 + \delta^2\eta^2)$.

If Bob chooses $\pm 2\theta$ phase shift of odd-parity check states for b_1 and b_2, Charlie chooses 0 phase shifts of even-parity check states for a_1 and a_2, c_1 and c_2, the state is

$$\begin{aligned} |\varphi_3\rangle_{a_1b_1c_1a_2b_2c_2} &= \alpha\delta(|HHV\rangle|HVV\rangle + |VHH\rangle|VVH\rangle) \\ &\quad +\beta\eta(|HVH\rangle|HHH\rangle + |VVV\rangle|VHV\rangle) \end{aligned} \tag{8}$$

with the probability $p_{11}^3 = 2(\alpha^2\delta^2 + \beta^2\eta^2)$.

If Bob chooses 0 phase shift of even-parity check state for b_1 and b_2, Charlie chooses $\pm 2\theta$ phase shift of odd-parity check states for c_1 and c_2, and 0 phase shift of even-parity check states for a_1 and a_2, the state is

$$\begin{aligned}|\varphi_4\rangle_{a_1b_1c_1a_2b_2c_2} &= \alpha\eta(|HHV\rangle|HHH\rangle + |VVV\rangle|VVH\rangle)\\ &\quad +\beta\delta(|HVH\rangle|HVV\rangle + |VHH\rangle|VHV\rangle)\end{aligned} \tag{9}$$

with the probability $p_{11}^4 = 2(\alpha^2\eta^2 + \beta^2\delta^2)$.

We give an example for PBSs measurement. After passing through HWP_{45°, $|\varphi_1\rangle_{a_1b_1c_1a_2b_2c_2}$ evolves into

$$\begin{aligned}\rightarrow\ & (\alpha^2|HHV\rangle + \beta^2|HVH\rangle + \delta^2|VHH\rangle + \eta^2|VVV\rangle)_{a_1b_1c_1}\\ & \times(|HHH\rangle + |VVV\rangle)_{a_2b_2c_2}\\ & +(\alpha^2|HHV\rangle - \beta^2|HVH\rangle - \delta^2|VHH\rangle + \eta^2|VVV\rangle)_{a_1b_1c_1}\\ & \times(|HHV\rangle + |VVH\rangle)_{a_2b_2c_2}\\ & +(-\alpha^2|HHV\rangle + \beta^2|HVH\rangle - \delta^2|VHH\rangle + \eta^2|VVV\rangle)_{a_1b_1c_1}\\ & \times(|HVH\rangle + |VHV\rangle)_{a_2b_2c_2}\\ & +(-\alpha^2|HHV\rangle - \beta^2|HVH\rangle + \delta^2|VHH\rangle + \eta^2|VVV\rangle)_{a_1b_1c_1}\\ & \times(|HVV\rangle + |VHH\rangle)_{a_2b_2c_2}.\end{aligned} \tag{10}$$

If the detectors $D_{A_1}, D_{B_1}, D_{C_1}$ (or $D_{A_2}, D_{B_2}, D_{C_2}$) are triggered, we will get

$$|\varphi_{11}^{(1)}\rangle_{a_1b_1c_1}^1 = \alpha^2|HHV\rangle + \beta^2|HVH\rangle + \delta^2|VHH\rangle + \eta^2|VVV\rangle, \tag{11}$$

where $\left|\varphi_{vj}^{(\gamma)}\right\rangle_{a_1b_1c_1}^m$ represents the quantum state with the number of rounds $v(v = 1, 2, 3, \ldots, k)$, the number of steps j ($j = 1, 2$) in vth round, the quantum state m ($m = 1, 2, 3, 4$) in jth step of vth round, and the quantum state (γ) ($\gamma = 1, 2, 3, 4$) of PBSs measurement for the states $|\varphi_\varepsilon\rangle_{a_1b_1c_1a_2b_2c_2}$ ($\varepsilon = 1, 2, 3, 4$).

If the detectors $D_{A_1}, D_{B_1}, D_{C_2}$ (or $D_{A_2}, D_{B_2}, D_{C_1}$) are triggered, we get

$$|\varphi_{11}^{(2)}\rangle_{a_1b_1c_1}^1 = \alpha^2|HHV\rangle - \beta^2|HVH\rangle - \delta^2|VHH\rangle + \eta^2|VVV\rangle. \tag{12}$$

Bob and Charlie perform unitary transformation $\sigma_z^B \otimes \sigma_z^A$ on photons a_1 and b_1 of state $|\varphi_{11}^{(2)}\rangle_{a_1b_1c_1}^1$ to get $|\varphi_{11}^{(1)}\rangle_{a_1b_1c_1}^1$.

If the detectors $D_{A_1}, D_{B_2}, D_{C_1}$ (or $D_{A_2}, D_{B_1}, D_{C_2}$) are triggered, we will get

$$|\varphi_{11}^{(3)}\rangle_{a_1b_1c_1}^1 = -\alpha^2|HHV\rangle + \beta^2|HVH\rangle - \delta^2|VHH\rangle + \eta^2|VVV\rangle. \tag{13}$$

Charlie performs unitary transformation $\sigma_z^A \otimes \sigma_z^C$ on photons a_1 and c_1 of state $|\varphi_{11}^{(3)}\rangle_{a_1b_1c_1}^1$ to get $|\varphi_{11}^{(1)}\rangle_{a_1b_1c_1}^1$.

If the detectors $D_{A_1}, D_{B_2}, D_{C_2}$ (or $D_{A_2}, D_{B_1}, D_{C_1}$) are triggered, we will get

$$|\varphi_{11}^{(4)}\rangle_{a_1b_1c_1}^1 = -\alpha^2|HHV\rangle - \beta^2|HVH\rangle + \delta^2|VHH\rangle + \eta^2|VVV\rangle. \tag{14}$$

Bob and Charlie perform unitary transformation $\sigma_z^B \otimes \sigma_z^C$ on photons b_1 and c_1 of state $|\varphi_{11}^{(4)}\rangle_{a_1b_1c_1}^1$ to get $|\varphi_{11}^{(1)}\rangle_{a_1b_1c_1}^1$.

For the three states $|\varphi_2\rangle_{a_1b_1c_1a_2b_2c_2}$, $|\varphi_3\rangle_{a_1b_1c_1a_2b_2c_2}$ and $|\varphi_4\rangle_{a_1b_1c_1a_2b_2c_2}$, we have the similar results

$$\begin{aligned}|\varphi_{11}^{(1)}\rangle_{a_1b_1c_1}^2 &= \alpha\beta(|HHV\rangle + |HVH\rangle) + \delta\eta(|VHH\rangle + |VVV\rangle),\\ |\varphi_{11}^{(1)}\rangle_{a_1b_1c_1}^3 &= \alpha\delta(|HHV\rangle + |VHH\rangle) + \beta\eta(|HVH\rangle + |VVV\rangle),\\ |\varphi_{11}^{(1)}\rangle_{a_1b_1c_1}^4 &= \alpha\eta(|HHV\rangle + |VVV\rangle) + \beta\delta(|HVH\rangle + |VHH\rangle).\end{aligned} \tag{15}$$

The four quantum states $|\varphi_{11}^{(1)}\rangle_{a_1b_1c_1}^1$, $|\varphi_{11}^{(1)}\rangle_{a_1b_1c_1}^2$, $|\varphi_{11}^{(1)}\rangle_{a_1b_1c_1}^3$ and $|\varphi_{11}^{(1)}\rangle_{a_1b_1c_1}^4$ are not destroyed by quantum non-demolition detections. They are used as the initial states in the second step of the first round and rewritten as $|\varphi_{12}\rangle_{a_1b_1c_1}^1$, $|\varphi_{12}\rangle_{a_1b_1c_1}^2$, $|\varphi_{12}\rangle_{a_1b_1c_1}^3$ and $|\varphi_{12}\rangle_{a_1b_1c_1}^4$.

In the second step, for quantum state

$$|\varphi_{12}\rangle_{a_1b_1c_1}^1 = \frac{1}{\sqrt{\alpha^4+\beta^4+\delta^4+\eta^4}}(\alpha^2|HHV\rangle + \beta^2|HVH\rangle + \delta^2|VHH\rangle + \eta^2|VVV\rangle), \tag{16}$$

photons are all flipped by HWP_{90° and relabeled as a_2, b_2 and c_2. We will get

$$|\varphi_{12}\rangle_{a_2b_2c_2}^1 = \frac{1}{\sqrt{\alpha^4+\beta^4+\delta^4+\eta^4}}(\alpha^2|VVH\rangle + \beta^2|VHV\rangle + \delta^2|HVV\rangle + \eta^2|HHH\rangle). \tag{17}$$

After parity checks and PBSs measurement, we obtain four quantum states

$$\begin{aligned}
|\varphi_{12}^{(1)}\rangle_{a_1b_1c_1}^1 &= \tfrac{1}{\alpha^4+\beta^4+\delta^4+\eta^4}[\alpha^4|HHV\rangle + \beta^4|HVH\rangle + \delta^4|VHH\rangle + \eta^4|VVV\rangle],\\
|\varphi_{12}^{(2)}\rangle_{a_1b_1c_1}^1 &= \tfrac{1}{\alpha^4+\beta^4+\delta^4+\eta^4}[\alpha^2\beta^2(|HHV\rangle + |HVH\rangle) + \delta^2\eta^2(|VHH\rangle + |VVV\rangle)],\\
|\varphi_{12}^{(3)}\rangle_{a_1b_1c_1}^1 &= \tfrac{1}{\alpha^4+\beta^4+\delta^4+\eta^4}[\alpha^2\delta^2(|HHV\rangle + |VHH\rangle) + \beta^2\eta^2(|HVH\rangle + |VVV\rangle)],\\
|\varphi_{12}^{(4)}\rangle_{a_1b_1c_1}^1 &= \tfrac{1}{\alpha^4+\beta^4+\delta^4+\eta^4}[\alpha^2\eta^2(|HHV\rangle + |VVV\rangle) + \beta^2\delta^2(|HVH\rangle + |VHH\rangle)].
\end{aligned} \tag{18}$$

The probabilities of getting quantum states $|\varphi_{12}^{(1)}\rangle_{a_1b_1c_1}^1$, $|\varphi_{12}^{(2)}\rangle_{a_1b_1c_1}^1$, $|\varphi_{12}^{(3)}\rangle_{a_1b_1c_1}^1$ and $|\varphi_{12}^{(4)}\rangle_{a_1b_1c_1}^1$ are

$$\begin{aligned}
p_{12}^1 &= \frac{\alpha^8+\beta^8+\delta^8+\eta^8}{(\alpha^4+\beta^4+\delta^4+\eta^4)^2},\\
p_{12}^2 &= \frac{2(\alpha^4\beta^4+\delta^4\eta^4)}{(\alpha^4+\beta^4+\delta^4+\eta^4)^2},\\
p_{12}^3 &= \frac{2(\alpha^4\delta^4+\beta^4\eta^4)}{(\alpha^4+\beta^4+\delta^4+\eta^4)^2},\\
p_{12}^4 &= \frac{2(\alpha^4\eta^4+\beta^4\delta^4)}{(\alpha^4+\beta^4+\delta^4+\eta^4)^2}.
\end{aligned} \tag{19}$$

These are all failed cases, but they can be used as the initial states in the second round.
For quantum state

$$|\varphi_{12}\rangle_{a_1b_1c_1}^2 = \tfrac{\alpha\beta}{\sqrt{2(\alpha^2\beta^2+\delta^2\eta^2)}}(|HHV\rangle + |HVH\rangle) + \tfrac{\delta\eta}{\sqrt{2(\alpha^2\beta^2+\delta^2\eta^2)}}(|VHH\rangle + |VVV\rangle), \tag{20}$$

its process of concentration is the same as $|\varphi_{12}\rangle_{a_1b_1c_1}^1$ and we can get

$$|\varphi_{12}^{(1)}\rangle_{a_1b_1c_1a_2b_2c_2}^2 = \tfrac{\alpha\beta\delta\eta}{2(\alpha^2\beta^2+\delta^2\eta^2)}(|HHV\rangle + |HVH\rangle + |VHH\rangle + |VVV\rangle). \tag{21}$$

This is the maximally GHZ entangled state. The success and failure probabilities of $|\varphi_{12}\rangle_{a_1b_1c_1}^2$ are

$$p_{12,s}^2 = \frac{2(\alpha\beta\delta\eta)^2}{(\alpha^2\beta^2+\delta^2\eta^2)^2}, \quad p_{12,f}^2 = \frac{\alpha^4\beta^4+\delta^4\eta^4}{(\alpha^2\beta^2+\delta^2\eta^2)^2}, \tag{22}$$

where the subscripts *s* and *f* represent the success and failure probabilities respectively.
For quantum states

$$\begin{aligned}
|\varphi_{12}\rangle_{a_1b_1c_1}^3 &= \tfrac{\alpha\delta}{\sqrt{2(\alpha^2\delta^2+\beta^2\eta^2)}}(|HHV\rangle + |VHH\rangle) + \tfrac{\beta\eta}{\sqrt{2(\alpha^2\delta^2+\beta^2\eta^2)}}(|HVH\rangle + |VVV\rangle),\\
|\varphi_{12}\rangle_{a_1b_1c_1}^4 &= \tfrac{\alpha\eta}{\sqrt{2(\alpha^2\eta^2+\beta^2\delta^2)}}(|HHV\rangle + |VVV\rangle) + \tfrac{\beta\delta}{\sqrt{2(\alpha^2\eta^2+\beta^2\delta^2)}}(|HVH\rangle + |VHH\rangle),
\end{aligned} \tag{23}$$

the success and failure probabilities of $|\varphi_{12}\rangle_{a_1b_1c_1}^3$ and $|\varphi_{12}\rangle_{a_1b_1c_1}^4$ are respectively

$$\begin{aligned}
p_{12,s}^3 &= \frac{2(\alpha\beta\delta\eta)^2}{(\alpha^2\delta^2+\beta^2\eta^2)^2}, \quad p_{12,f}^3 = \frac{\alpha^4\delta^4+\beta^4\eta^4}{(\alpha^2\delta^2+\beta^2\eta^2)^2},\\
p_{12,s}^4 &= \frac{2(\alpha\beta\delta\eta)^2}{(\alpha^2\eta^2+\beta^2\delta^2)^2}, \quad p_{12,f}^4 = \frac{\alpha^4\eta^4+\beta^4\delta^4}{(\alpha^2\eta^2+\beta^2\delta^2)^2}.
\end{aligned} \tag{24}$$

The total success probability of the first round is

$$\begin{aligned}
P_1 &= p_{11}^2p_{12,s}^2 + p_{11}^3p_{12,s}^3 + p_{11}^4p_{12,s}^4\\
&= \frac{4(\alpha\beta\delta\eta)^2}{\alpha^2\beta^2+\delta^2\eta^2} + \frac{4(\alpha\beta\delta\eta)^2}{\alpha^2\delta^2+\beta^2\eta^2} + \frac{4(\alpha\beta\delta\eta)^2}{\alpha^2\eta^2+\beta^2\delta^2}.
\end{aligned} \tag{25}$$

Discussion

Blindness and correctness analysis of the proposed BQC protocol. In the following, we will show that the proposed BQC protocol is secure by analyzing the blindness and correctness.

First, we show the blindness of the proposed BQC protocol.

(1) Bob performs one of four Pauli operations randomly chosen by Alice on his photons and the initial states $|GHZ\rangle_{A'_{t_2}B_jC'_{t_1}} = \frac{1}{2}(|001\rangle + |010\rangle + |100\rangle + |111\rangle)$ are correspondingly changed into one of

$\{|GHZ_1\rangle_{A'_{t_2}B_jC'_{t_1}}, |GHZ_2\rangle_{A'_{t_2}B_jC'_{t_1}}, |GHZ_3\rangle_{A'_{t_2}B_jC'_{t_1}}, |GHZ_4\rangle_{A'_{t_2}B_jC'_{t_1}}\}$. Whether Bob colludes with Charlie or not, they guess the correct Bell state with the probability of $\frac{1}{4}$. When this BQC protocol is repeated n times, the probability of obtaining correct quantum states is $\lim_{n\to\infty}\left(\frac{1}{4}\right)^n = 0$.

(2) Alice randomly chooses the phase $\theta_i \in \left\{0, \frac{\pi}{4}, \frac{2\pi}{4}, \frac{3\pi}{4}, \ldots, \frac{7\pi}{4}\right\}$ and disturbs the order of photons A_j, B_j, C_j. Bob and Charlie know nothing about the states $|\pm_{\theta_i}\rangle$ because of the no-signaling principle. After repeating n times, the probability of guessing correct θ_i is $\lim_{n\to\infty}\left(\frac{1}{8}\right)^n = 0$. In the process of entanglement concentration, Bob and Charlie cannot eavesdropping any useful information by exchanging their results because of difference of orders of three photons.

(3) The structures of blind brickwork states and blind topological states are private for servers. Therefore, Bob and Charlie can't obtain anything about Alice's private information whether they communicate with each other or not. The blindness of BFK single-server protocol and blind topological single-server protocol are showed in refs 1 and 2 in detail respectively.

Second, the correctness of quantum computation in BFK single-server protocol and blind topological single-server protocol are presented in refs 1 and 2 in detail.

So this BQC protocol is blind and correct.

Analysis of the success probabilities in iteration. In the above discussion, we have already elaborated the first round of the entanglement concentration with cross-Kerr nonlinearity in detail. QND provides a strong tool for us to perform a quantum nondemolition measurement that does not destroy entanglement of photons, which ensures that each step can be operated independently. Here, we analyse the second round and the k-th round of entanglement concentration.

For the three cases $|\varphi_{21}\rangle^2_{a_1b_1c_1}$, $|\varphi_{21}\rangle^3_{a_1b_1c_1}$ and $|\varphi_{21}\rangle^4_{a_1b_1c_1}$, only the first step is needed to concentrate the ideal maximally entangled states $|GHZ\rangle_{A'_{t_2}B_jC'_{t_1}}$. However, we need to implement two steps for the state $|\varphi_{21}\rangle^1_{a_1b_1c_1}$. We consider the three states $|\varphi_{21}\rangle^2_{a_1b_1c_1}$, $|\varphi_{21}\rangle^3_{a_1b_1c_1}$ and $|\varphi_{21}\rangle^4_{a_1b_1c_1}$ first.

In the second round, for the quantum states

$$|\varphi_{21}\rangle^2_{a_1b_1c_1} = \frac{\alpha^2\beta^2}{\sqrt{2(\alpha^4\beta^4+\delta^4\eta^4)}}(|HHV\rangle + |HVH\rangle) + \frac{\delta^2\eta^2}{\sqrt{2(\alpha^2\beta^4+\delta^4\eta^4)}}(|VHH\rangle + |VVV\rangle), \tag{26}$$

its analysis is the same as the Eq. (20). The success and failure probabilities are

$$p^2_{21,s} = \frac{2(\alpha\beta\delta\eta)^4}{(\alpha^4\beta^4+\delta^4\eta^4)^2}, \quad p^2_{21,f} = \frac{\alpha^8\beta^8+\delta^8\eta^8}{(\alpha^4\beta^4+\delta^4\eta^4)^2}. \tag{27}$$

In the k-th ($k>1$) round, the success and failure probabilities are

$$p^2_{k1,s} = \frac{2(\alpha\beta\delta\eta)^{2^k}}{(\alpha^{2^k}\beta^{2^k}+\delta^{2^k}\eta^{2^k})^2}, \quad p^2_{k1,f} = \frac{\alpha^{2^{k+1}}\beta^{2^{k+1}}+\delta^{2^{k+1}}\eta^{2^{k+1}}}{(\alpha^{2^k}\beta^{2^k}+\delta^{2^k}\eta^{2^k})^2}. \tag{28}$$

For the quantum states

$$|\varphi_{21}\rangle^3_{a_1b_1c_1} = \frac{\alpha^2\delta^2}{\sqrt{2(\alpha^4\delta^4+\beta^4\eta^4)}}(|HHV\rangle + |VHH\rangle) + \frac{\beta^2\eta^2}{\sqrt{2(\alpha^4\delta^4+\beta^4\eta^4)}}(|HVH\rangle + |VVV\rangle),$$
$$|\varphi_{21}\rangle^4_{a_1b_1c_1} = \frac{\alpha^2\eta^2}{\sqrt{2(\alpha^4\eta^4+\beta^4\delta^4)}}(|HHV\rangle + |VVV\rangle) + \frac{\beta^2\delta^2}{\sqrt{2(\alpha^4\eta^4+\beta^4\delta^4)}}(|HVH\rangle + |VHH\rangle),$$

the analyses of entanglement concentration are the same as the Eq. (23), the success and failure probabilities in the second round and the k-th round are

$$\begin{aligned}
p^3_{21,s} &= \frac{2(\alpha\beta\delta\eta)^4}{(\alpha^4\delta^4+\beta^4\eta^4)^2}, \quad p^3_{k1,s} = \frac{2(\alpha\beta\delta\eta)^{2^k}}{(\alpha^{2^k}\delta^{2^k}+\beta^{2^k}\eta^{2^k})^2},\\
p^3_{21,f} &= \frac{\alpha^8\delta^8+\beta^8\eta^8}{(\alpha^4\delta^4+\beta^4\eta^4)^2}, \quad p^3_{k1,f} = \frac{\alpha^{2^{k+1}}\delta^{2^{k+1}}+\beta^{2^{k+1}}\eta^{2^{k+1}}}{(\alpha^{2^k}\delta^{2^k}+\beta^{2^k}\eta^{2^k})^2},\\
p^4_{21,s} &= \frac{2(\alpha\beta\delta\eta)^4}{(\alpha^4\eta^4+\beta^4\delta^4)^2}, \quad p^4_{k1,s} = \frac{2(\alpha\beta\delta\eta)^{2^k}}{(\alpha^{2^k}\eta^{2^k}+\beta^{2^k}\delta^{2^k})^2},\\
p^4_{21,f} &= \frac{\alpha^8\eta^8+\beta^8\delta^8}{(\alpha^4\eta^4+\beta^4\delta^4)^2}, \quad p^4_{k1,f} = \frac{\alpha^{2^{k+1}}\eta^{2^{k+1}}+\beta^{2^{k+1}}\delta^{2^{k+1}}}{(\alpha^{2^k}\eta^{2^k}+\beta^{2^k}\delta^{2^k})^2}.
\end{aligned} \tag{29}$$

For the quantum states

$$|\varphi_{kj}\rangle^1_{a_1b_1c_1} = \alpha_{kj}|HHV\rangle + \beta_{kj}|HVH\rangle + \delta_{kj}|VHH\rangle + \eta_{kj}|VVV\rangle, \tag{30}$$

(where $j = 1, 2$) we give the relevant normalized coefficients and the probabilities of relevant quantum states. The iterative process is the same as the Eq. (3).

In the first step of the k-th round, for the quantum states

$$|\varphi_{k1}\rangle^1_{a_1b_1c_1} = \alpha_{k1}|HHV\rangle + \beta_{k1}|HVH\rangle + \delta_{k1}|VHH\rangle + \eta_{k1}|VVV\rangle, \tag{31}$$

where $k > 1$ and the coefficients are

$$\begin{aligned}
\alpha_{k1} &= \frac{\alpha^{2^{2k-2}}}{\sqrt{\alpha^{2^{2k-1}} + \beta^{2^{2k-1}} + \delta^{2^{2k-1}} + \eta^{2^{2k-1}}}},\\
\beta_{k1} &= \frac{\beta^{2^{2k-2}}}{\sqrt{\alpha^{2^{2k-1}} + \beta^{2^{2k-1}} + \delta^{2^{2k-1}} + \eta^{2^{2k-1}}}},\\
\delta_{k1} &= \frac{\delta^{2^{2k-2}}}{\sqrt{\alpha^{2^{2k-1}} + \beta^{2^{2k-1}} + \delta^{2^{2k-1}} + \eta^{2^{2k-1}}}},\\
\eta_{k1} &= \frac{\eta^{2^{2k-2}}}{\sqrt{\alpha^{2^{2k-1}} + \beta^{2^{2k-1}} + \delta^{2^{2k-1}} + \eta^{2^{2k-1}}}}.
\end{aligned} \tag{32}$$

In the second step of the k-th round, for the quantum states

$$|\varphi_{k2}\rangle^1_{a_1b_1c_1} = \alpha_{k2}|HHV\rangle + \beta_{k2}|HVH\rangle + \delta_{k2}|VHH\rangle + \eta_{k2}|VVV\rangle, \tag{33}$$

where the coefficients are

$$\begin{aligned}
\alpha_{k2} &= \frac{\alpha^{2^{2k-1}}}{\sqrt{\alpha^{2^{2k}} + \beta^{2^{2k}} + \delta^{2^{2k}} + \eta^{2^{2k}}}},\\
\beta_{k2} &= \frac{\beta^{2^{2k-1}}}{\sqrt{\alpha^{2^{2k}} + \beta^{2^{2k}} + \delta^{2k} + \eta^{2^{2k}}}},\\
\delta_{k2} &= \frac{\delta^{2^{2k-1}}}{\sqrt{\alpha^{2^{2k}} + \beta^{2^{2k}} + \delta^{2^{2k}} + \eta^{2^{2k}}}},\\
\eta_{k2} &= \frac{\eta^{2^{2k-1}}}{\sqrt{\alpha^{2^{2k}} + \beta^{2^{2k}} + \delta^{2^{2k}} + \eta^{2^{2k}}}}.
\end{aligned} \tag{34}$$

The probabilities of obtaining four quantum states in the first step or the second step of the k-th round are

$$\begin{aligned}
p^1_{kj} &= \alpha^4_{kj} + \beta^4_{kj} + \delta^4_{kj} + \eta^4_{kj},\\
p^2_{kj} &= 2(\alpha^2_{kj}\beta^2_{kj} + \delta^2_{kj}\eta^2_{kj}),\\
p^3_{kj} &= 2(\alpha^2_{kj}\delta^2_{kj} + \beta^2_{kj}\eta^2_{kj}),\\
p^4_{kj} &= 2(\alpha^2_{kj}\eta^2_{kj} + \beta^2_{kj}\delta^2_{kj}),
\end{aligned} \tag{35}$$

where $j = 1, 2$. The success probability of the kth round is

$$\begin{aligned}
P_k \;=\; & p^2_{11}p^2_{12,f}p^2_{21,f}p^2_{31,f}\cdots p^2_{(k-1)1,f}p^2_{k1,s}\\
& + p^3_{11}p^3_{12,f}p^3_{21,f}\cdots p^3_{(k-1)1,f}p^3_{k1,s}\\
& + p^4_{11}p^4_{12,f}p^4_{21,f} + \cdots p^4_{(k-1)1,f}p^4_{k1,s}\\
& + p^1_{11}(p^2_{12}p^2_{21,f}p^2_{31,f}\cdots p^2_{(k-1)1,f}p^2_{k1,s}\\
& + p^3_{12}p^3_{21,f}p^3_{31,f}\cdots p^3_{(k-1)1,f}p^3_{k1,f}\\
& + p^4_{12}p^4_{21,f}p^4_{31,f}\cdots p^4_{(k-1)1,f}p^4_{k1,f})\\
& + \cdots + p^1_{11}p^1_{12}p^1_{21}p^1_{22}p^1_{31}p^1_{32}\cdots p^1_{(k-1)1}p^1_{(k-1)2}(p^2_{k1}p^2_{k2,s} + p^3_{k1}p^3_{k2,s} + p^4_{k1}p^4_{k2,s}).
\end{aligned} \tag{36}$$

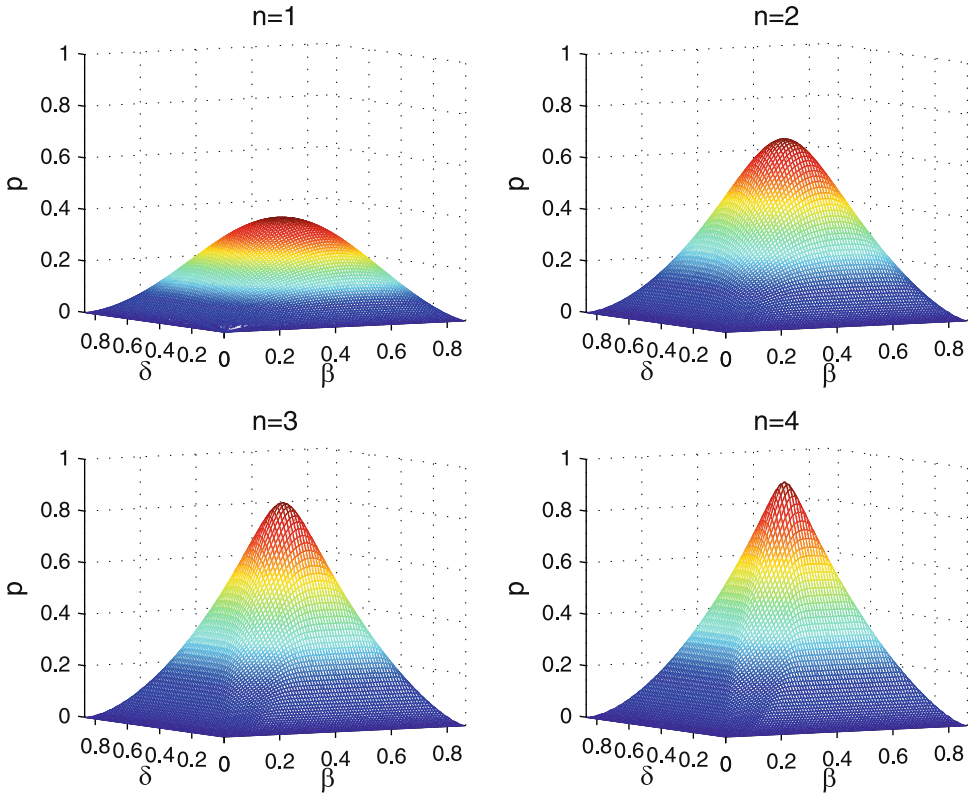

Figure 4. The success probability P of getting maximally entangled GHZ state relies on the initial coefficients β and δ. Here, we let $\alpha = \frac{1}{2}, \beta \in \{0, \frac{\sqrt{3}}{2}\}, \delta \in \{0, \sqrt{\frac{3}{4} - \beta^2}\}, \eta = \sqrt{\frac{3}{4} - \beta^2 - \delta^2}$. n ($n = 1, 2, 3, 4$) represents the number of iterations.

The total probability is $P_{total} = \sum_{k=1}^{n} P_k$, which depends on the number of iterations and parameters of the initial states. The relationship of the total success probability, parameters and the number of iterations is shown in Fig. 4. It can be seen that the total success probability has kept increasing with the parameters β and δ in the range of $\left[0, \frac{\sqrt{3}}{2}\right]$. When $n = 4$, the success probability has already reached 0.9196. When $n = 9$, the success probability has already reached 0.9975. Therefore, the entanglement concentration is successful in theory.

In this paper, we only consider the ideal CNOT gate[19–23]. In experiment, there exist many nonideal factors such as the double effect of parameter conversion, the imperfect matching of the crystal lattice and phases, and so on. The probabilities of intrinsic error of experimental methods are unavoidable, such as QND measurements and CNOT operations. Thus optimizing the experimental system is a very meaningful research direction. In the BQC protocol, we only give the concrete quantum channel noise model but not universal. So, we will further study entanglement purification of GHZ states.

Methods

The optical devices are used to complete the entanglement concentration, where the parity check devices are based on cross-Kerr nonlinearity that can construct QND[38, 39, 41] to improve the successful probability. The cross-Kerr nonlinearity medium is described by the Hamiltonian,

$$H = \hbar\chi a_s^\dagger a_s a_p^\dagger a_p \tag{37}$$

where $a_s^\dagger$ and $a_p^\dagger$ are the creation operators, a_s and a_p are the annihilation operators, a Fock state $|n\rangle$ and a coherent state $|\alpha_c\rangle$ interact. The whole system evolves into

$$U(t)|n\rangle|\alpha_c\rangle = c_0|0\rangle|\alpha_c\rangle + c_1|1\rangle|\alpha_c e^{i\theta}\rangle \tag{38}$$

where $U(t) = e^{-i\theta a_s^\dagger a_s a_p^\dagger a_p}$, $\theta = \chi t$ is the phase shift and t is the interaction time ($c = 1, 2, 3$). θ is proportional to the number of photons in the signal state $|\alpha_c\rangle$. X-quadrature measurement can recognize the phase shift of signal states $|\alpha_c\rangle$. The cross-Kerr nonlinearity can measure the number of photons but do not destroy the photons.

For the parity check device in Fig. 3, we give an example. Two polarization photons are initially prepared with the forms of $|\tau\rangle_{k_1} = \mu_0|H\rangle + \mu_1|V\rangle$ and $|\tau\rangle_{k_2} = \lambda_0|H\rangle + \lambda_1|V\rangle$ that interact with a coherent beam $|\alpha_c\rangle$ ($c = 1, 2, 3$), where real numbers μ_0, μ_1, λ_0 and λ_1 satisfy the normalization condition $|\mu_0|^2 + |\mu_1|^2 = 1$, $|\lambda_0|^2 + |\lambda_1|^2 = 1$, respectively. Then the composite quantum system $|\Upsilon_1\rangle = |\tau\rangle_{k_1} \otimes |\tau\rangle_{k_2} \otimes |\alpha_c\rangle$ evolves to

$$|\Upsilon_2\rangle = \mu_0\lambda_1|HV\rangle|\alpha_c e^{-2i\theta}\rangle + \mu_1\lambda_0|VH\rangle|\alpha_c e^{2i\theta}\rangle + (\mu_0\lambda_0|HH\rangle + \mu_1\lambda_1|VV\rangle)|\alpha_c\rangle \quad (39)$$

From the Eq. (39), we can pick up a phase shift 0 related with $|HH\rangle$ and $|VV\rangle$, and phase shift 2θ related with $|HV\rangle$ and $|VH\rangle$. One can distinguish $|HH\rangle$ and $|VV\rangle$ from $|HV\rangle$ and $|VH\rangle$ by different phase shifts, however, the states $|\alpha_1 e^{\mp 2i\theta}\rangle$ can not be distinguished by the setup.

References

1. Broadbent, A., Fitzsimons, J. & Kashefi, E. Universal blind quantum computation. In *Proceedings of the 50th Annual IEEE Symposium on Foundations of Computer Science* 517–526 (IEEE Computer society, Los Alamitos, USA, 2009).
2. Morimae, T. & Fujii, K. Blind topological measurement-based quantum computation. *Nat. Commun.***3**, 1–6 (2012).
3. Morimae, T., Dunjko, V. & Kashefi, E. Ground state blind quantum computation on AKLT state. *Quantum Inf. Computat.***15**, 200–234 (2015).
4. Morimae, T. & Fujii, K. Secure entanglement distillation for double-server blind quantum computation. *Phys. Rev. Lett.***111**, 020502 (2013).
5. Li, Q., Chan, W. H., Wu, C. H. & Wen, Z. H. Triple-server blind quantum computation using entanglement swapping. *Phys. Rev. A***89**, 040302(R) (2014).
6. Sheng, Y. B. & Zhou, L. Deterministic entanglement distillation for secure double-server blind quantum computation. *Sci. Rep.***5**, 7815 (2015).
7. Barz, S., Kashefi, E., Broadbent, A., Fitzsimons, J. F. & Zeilinger, A. Demonstration of blind quantum computing. *Science***335**, 303–308 (2012).
8. Darmawan, A. S. & Bartlett, S. D. Optical spin-1 chain and its use as a quantum-computational wire. *Phys. Rev. A***82**, 012328 (2010).
9. Hayashi, M. & Morimae, T. Verifiable measurement-only blind quantum computing with stabilizer testing. *Phys. Rev. Lett.***115**, 220502 (2015).
10. Morimae, T. Verification for measurement-only blind quantum computing. *Phys. Rev. A***89**, 060302(R) (2014).
11. Greganti, C., Roehsner, M. C., Barz, S., Morimae, T. & Walthe, P. Demonstration of measurement-only blind quantum computing. *New J. Phys.***18**, 013020 (2016).
12. Takeuchi, Y., Fujii, K., Morimae, T. & Imoto, N. *Practically verifiable blind quantum computation with acceptance rate amplification*. Preprint at arXiv:1607.01568v1 (2016).
13. Morimae, T. *Measurement-only verifiable blind quantum computing with quantum input verification*. Preprint at arXiv:1606.06467v1 (2016).
14. Takeuchi, Y., Fujii, K., Ikuta, R., Yamamoto, T. & Imoto, N. Blind quantum computation over a collective-noise channel. *Phys. Rev. A***93**, 052307 (2016).
15. Pérez-Delgado, C. A. & Fitzsimons, J. F. Iterated gate teleportation and blind quantum computation. *Phys. Rev. Lett.***114**, 220502 (2015).
16. Morimae, T. Continuous-variable blind quantum computation. *Phys. Rev. Lett.***109**, 230502 (2012).
17. Sueki, T., Koshiba, T. & Morimae, T. Ancilla-driven universal blind quantum computation. *Phys. Rev. A***87**, 060301(R) (2013).
18. Morimae, T. & Fujii, K. Blind quantum computation protocol in which Alice only makes measurements. *Phys. Rev. A***87**, 050301(R) (2013).
19. Nemoto, K. & Munro, W. J. Nearly Deterministic Linear Optical Controlled-NOT Gate. *Phys. Rev. Lett.***93**, 250502 (2004).
20. Pittman, T. B., Jacobs, B. C. & Franson, J. D. Probabilistic quantum logic operations using polarizing beam splitters. *Phys. Rev. A***64**, 062311 (2001).
21. DeMarco, B. *et al*. Experimental Demonstration of a Controlled-NOT Wave-Packet Gate. *Phys. Rev. Lett.***89**, 267901 (2002).
22. Zhao, Z. *et al*. Experimental Demonstration of a Nondestructive Controlled-NOT Quantum Gate for Two Independent Photon Qubits. *Phys. Rev. Lett.***94**, 030501 (2005).
23. Testolin, M. J., Hill, C. D., Wellard, C. J. & Hollenberg, L. C. L. Robust controlled-NOT gate in the presence of large fabrication-induced variations of the exchange interaction strength. *Phys. Rev. A***76**, 012302 (2007).
24. Bennett, C. H. *et al*. Purification of Noisy Entanglement and Faithful Teleportation via Noisy Channels. *Phys. Rev. Lett.***76**, 722 (1996).
25. Pan, J. W., Simon, C. & Zeillinger, A. Entanglement purification for quantum communication. *Nature (London)***410**, 1067 (2001).
26. Pan, J. W., Gasparonl, S., Ursin, R., Weihs, G. & Zeillinger, A. Experimental entanglement purification of arbitrary unknown states. *Nature (London)***423**, 417 (2003).
27. Sheng, Y. B. & Deng, F. G. One-step deterministic polarization-entanglement purification using spatial entanglement. *Phys. Rev. A***82**, 044305 (2010).
28. Sheng, Y. B. & Deng, F. G. Deterministic entanglement purification and complete nonlocal Bell-state analysis with hyperentanglement. *Phys. Rev. A***81**, 032307 (2010).
29. Bennett, C. H., Bernstein, H. J., Popescu, S. & Schumacher, B. Concentrating partial entanglement by local operations. *Phys. Rev. A***53**, 2046–2052 (1996).
30. Zhao, Z., Pan, J. W. & Zhan, M. S. Practical scheme for entanglement concentration. *Phys. Rev. A***64**, 014301 (2001).
31. Sheng, Y. B., Deng, F. G. & Zhou, H. Y. Nonlocal entanglement concentration scheme for partially entangled multipartite systems with nonlinear optics. *Phys. Rev. A***77**, 062325 (2008).
32. Sheng, Y. B., Zhou, L. & Zhao, S. M. Efficient two-step entanglement concentration for arbitrary W states. *Phys. Rev. A***85**, 042302 (2012).
33. Du, F. F., Li, T., Ren, B. C., Wei, H. R. & Deng, F. G. Single-photon-assisted entanglement concentration of a multiphoton system in a partially entangled W state with weak cross-Kerr nonlinearity. *J. Opt. Soc. Am. B***29**, 1399–1405 (2012).
34. Gu, B. Single-photon-assisted entanglement concentration of partially entangled multiphoton W states with linear optics. *J. Opt. Soc. Am. B***29**, 1685–1689 (2012).
35. Wang, T. J. & Long, G. L. Entanglement concentration for arbitrary unknown less-entangled three-photon W states with linear optics. *J. Opt. Soc. Am. B***30**, 1069–1076 (2013).
36. Zhou, L., Sheng, Y. B. & Zhao, S. M. Optimal entanglement concentration for three-photon W states with parity check measurement. *Chin. Phys. B***22**, 020307 (2013).
37. He, B. & Bergou, J. A. Entanglement transformation with no classical communication. *Phys. Rev. A***78**, 062328 (2008).
38. Deng, F. G. Optimal nonlocal multipartite entanglement concentration based on projection measurements. *Phys. Rev. A***85**, 022311 (2012).
39. Li, X. H. & Ghose, S. Efficient hyperconcentration of nonlocal multipartite entanglement via the cross-Kerr nonlinearity. *Opt. Express***23**, 3550–3562 (2015).
40. Li, X. H., Chen, X. & Zeng, Z. Hyperconcentration for entanglement in two degrees of freedom. *J. Opt. Soc. Am. B***30**, 2774–2780 (2013).

41. Sheng, Y. B., Zhou, L., Zhao, S. M. & Zhang, B. Efficient single-photon-assisted entanglement concentration for partially entangled photon pairs. *Phys. Rev. A***85**, 012307 (2012).
42. Zhao, Z. *et al*. Experimental Realization of Entanglement Concentration and a Quantum Repeater. *Phys. Rev. Lett.***90**, 207901 (2009).
43. Sheng, Y. B., Pan, J., Guo, R., Zhou, L. & Wang, L. Efficient N-particle W state concentration with different parity check gates. *Sci. China Phys. Mech.***58**, 060301 (2015).
44. Du, F. F. & Deng, F. G. Heralded entanglement concentration for photon systems with linear-optical elements. *Sci. China Phys. Mech.***58**, 040303 (2015).
45. Cao, C. *et al*. Concentrating partially entangled W-class states on nonlocal atoms using low-Q optical cavity and linear optical elements. *Sci. China Phys. Mech.***59**, 100315 (2016).
46. Xia, Y., Song, J. & Song, H. S. Remote preparation of the N-particle GHZ state using quantum statistics. *Opt. Commun.***277**, 219–222 (2007).
47. Bishop, LevS. *et al*. Proposal for generating and detecting multi-qubit GHZ states in circuit QED. *New J. Phys.***11**, 073040 (2009).
48. Bouwmeester, D., Pan, J. W., Daniell, M., Weinfurter, H. & Zeilinger, A. Observation of Three-Photon Greenberger-Horne-Zeilinger Entanglement. *Phys. Rev. Lett.***82**, 1345–1349 (1999).
49. Sheng, Y. B., Guo, R., Pan, J., Zhou, L. & Wang, X. F. Two-step measurement of the concurrence for hyperentangled state. *Quantum Inf. Process***14**, 963–978 (2015).

Acknowledgements

This work was supported by National Science Foundation of China (Grant Nos 61472165, 61373158, 61672014 and 61502200), Guangdong Provincial Engineering Technology Research Center on Network Security Detection and Defence (Grant No. 2014B090904067), Guangdong Provincial Special Funds for Applied Technology Research and development and Transformation of Important Scientific and Technological Achieve (Grant No. 2016B010124009), the Zhuhai Top Discipline–Information SecurityGuangzhou Key Laboratory of Data Security and Privacy Preserving, Guangdong Key Laboratory of Data Security and Privacy Preserving, the Transformation Project of Sci-tech Achievements of SYSU, Natural Science Foundation of Guangdong Province, China, under Grant Nos 2016A030313090 and 2014A030310245, and Science and Technology Planning Project of Guangdong Province, China, under Grant No. 2013B010401018, Special Program for Applied Research on Super Computation of the NSFC-Guangdong Joint Fund (the second phase) (No. nsfc2015_180), the Natural Science Foundation of Guangdong (No. 2016A030313350), the Special Funds for Science and Technology Development of Guangdong (No. 2016KZ010103), the Fundamental Research Funds for the Central Universities (No. 16lgjc83), and Scientific and Technological Achievements Transformation Plan of Sun Yat-sen University.

Author Contributions

X.Q. Zhang and J. Weng proposed and wrote the main manuscript text. J. Weng, W. Lu, X.C. Li, W.Q. Luo and X.Q. Tan reviewed the manuscript. J. Weng, W. Lu and X.Q. Tan provided funding support.

Additional Information

Competing Interests: The authors declare that they have no competing interests.

Publisher's note: Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.