Photonic spatial Bell-state analysis for robust quantum secure direct communication using quantum dot-cavity systems

Bao-Cang Ren, Hai-Rui Wei, Ming Hua, Tao Li, and Fu-Guo Deng†
Department of Physics, Applied Optics Beijing Area Major Laboratory,
Beijing Normal University, Beijing 100875, China
(Dated: April 2, 2013)

Recently, experiments showed that the spatial-mode states of entangled photons are more robust than their polarization-mode states in quantum communications. Here we construct a complete and deterministic protocol for analyzing the spatial Bell states using the interaction between a photon and an electron spin in a charged quantum dot inside a one-side micropillar microcavity. A quantum nondemolition detector (QND) for checking the parity of a two-photon system can be constructed with the giant optical Faraday rotation in this solid state system. With this parity-check QND, we present a complete and deterministic proposal for the analysis of the four spatial-mode Bell states. Moreover, we present a robust two-step quantum secure direct communication protocol based on the spatial-mode Bell states and the photonic spatial Bell-state analysis. Our analysis shows that our BSA proposal works in both the strong and the weak coupling regimes if the side leakage and cavity loss rate is small.

PACS numbers: 03.67.Hk—Quantum communication, 12.20.-m—Quantum electrodynamics, 78.67.Hc—Quantum dots

I. INTRODUCTION

Entanglement, an essential quantum correlation between two quantum subsystems [1, 2], lies at the heart of quantum information and it plays a critical role in quantum information processing, especially for quantum computation [1], quantum key distribution (QKD) [3–7], quantum teleportation [8], entanglement swapping [9], quantum dense coding [10, 11], quantum secret sharing (QSS) [12–14], and so on. In most quantum communication tasks, Bell-state analysis (BSA) is required, especially in teleportation, entanglement swapping, dense coding, quantum state sharing [15–19], and quantum repeaters. BSA is defined as the projection of the state of a two-qubit system onto the maximally entangled Bell states. The four Bell states of two-qubit systems are orthogonal to each other and are deemed to be discriminated deterministically in principle, but BSA is always a technical difficulty, which yields a low efficiency and a low discrimination fidelity [20]. It is impossible to distinguish the four Bell states in the polarization degree of freedom (DOF) with only linear optical elements. In 1999, Vaidman’s [21] and Lütkenhaus’ [22] groups put forward a BSA protocol for teleportation with the success probability of $\frac{1}{2}$, resorting to only linear optical elements. In the following years, some other proposals to analyze completely Bell states in the polarization DOF, including those using spatial entanglement of photons, were introduced [23–30]. The complete BSA on the polarization DOF requires the hyperentanglement in both the polarization DOF and the spatial DOF (or another DOF) or the nonlinear interaction between photons and media.

Recent works showed that an electron spin in a charged quantum dot (QD) inside a microwave cavity [31] can be used to store and process quantum information. In 2008, Hu et al. [32] proposed a quantum nondemolition method using the interaction of the left-circularly and the right-circularly polarized lights with a QD-cavity system. This giant circular birefringence (GCB) in a QD-cavity system can be used to construct a CNOT gate [33], a multiphoton entangler [34, 35], a photonic polarization Bell-state analyzer [36], entanglement purification [37], and so on.

In 2000, Long and Liu [38] proposed an interesting quantum communication protocol with a quantum data block, which can be used to transmit the secret message directly between two legitimate users (without creating a private key first). It was detailed and given the term as quantum secure direct communication (QSDC) by Deng, Long, and Liu [39] in 2003. Subsequently, QSDC was actively pursued by some groups and people proposed some QSDC protocols [38, 51], quasi-secure quantum communication protocols [52], and some deterministic secure quantum communication protocols [53, 54]. In most of QSDC protocols existing, the polarization states of photon systems are used to carry the secret message [60]. However, the polarization states of photons are fragile to channel noise when they are transmitted over a practical channel, such as an optical fiber or a free space. Fortunately, some DOFs of photon systems are robust against channel noise, such as the spatial-mode DOF and the frequency DOF of photon systems. For example, the entanglement in the spatial-mode DOF of photon pairs was used to purify the entanglement in the polarization DOF by people [61, 62]. The experiment showed [62] that it is not more difficult to control the stability of the spatial
entanglement. In 2008, the experiment by Minář et al. for phase-noise measurements showed that the phase in long fibers with several tens of km remains stable in a realistic environment, which is an acceptable level for time on the order of 100 µs and is enough for the phase stabilization in feasible quantum repeaters with optical-fiber networks. Also, the frequency entanglement is used for faithful entanglement distribution on the polarization entanglement of photon pairs. In 1999, Merolla et al. showed that a quantum bit error rate contribution of approximately 4% and estimated that 2% could be attributed to the transmission of the central frequency by the Fabry-Perot cavity in a key distribution experiment over a 20-km single-mode optical-fiber spool. However, the Hadamard operation on the frequency states of photons is difficult, which limits the direct application of frequency entanglement in quantum communication, different from the spatial entanglement of photon systems.

In this paper, we present a complete and deterministic analysis protocol for the photonic spatial Bell states, resorting to the GCB based on a quantum dot inside a one-side micropillar microcavity. In our proposal, we first construct a parity-check quantum nondemolition detector (QND) for the spatial-mode DOF of photon pairs by exploiting the interaction between a photon and an electron spin in a charged quantum dot (QD) inside a one-side micropillar microcavity. With this QND, we can first divide the four Bell states in spatial-mode DOF into two groups, that is, the even-parity group and the odd-parity group, according to their parities of the two photons in the spatial-mode DOF, and then distinguish the relative phase of the two states in each group by transforming the difference of the phases into that of the spatial modes with BSs and QND. Based on the spatial-mode Bell states and their BSA, we present a robust two-step quantum secure direct communication protocol as the spatial entanglement of two-photon systems is more robust than the polarization entanglement. Our analysis shows that our BSA proposal for spatial-mode Bell states works in both the strong coupling regime and the weak coupling regime if the side leakage and cavity loss rate is small.

II. QD-CAVITY SYSTEM

In order to understand the principle of the interaction between a photon and an electron spin, we first introduce the construction of a one-side QD-cavity system. The QD-cavity system is always constructed by a singly charged QD (self-assembled In(Ga)As QD or a GaAs interface QD) located in the center of a one-side optical resonant cavity for maximal light-matter coupling. If an excess electron is injected into the singly charged QD, a negatively charged exciton \( (X^-) \) with two electrons bound to one hole \([\tilde{1}1]\) is created by optical excitation. Different excess electron spins create different structures of \( X^- \), according to Pauli’s exclusion principle, which is called \( X^- \) spin-dependent transitions. If the injected excess electron spin is in the state \(|\uparrow\rangle\), the QD-cavity system resonantly absorbs a left-handed circularly polarized light \(|L\rangle\) and creates a negatively charged exciton in the state \(|\uparrow\downarrow\rangle\). If the injected excess electron spin is in the state \(|\downarrow\rangle\), the QD-cavity system resonantly absorbs a right-handed circularly polarized light \(|R\rangle\) and creates a negatively charged exciton in the state \(|\downarrow\uparrow\rangle\). Here, \(|\uparrow\rangle\) and \(|\downarrow\rangle\) represent the heavy-hole spin states \(|\frac{3}{2}\rangle\) and \(|-\frac{3}{2}\rangle\), respectively.

The \( X^- \) spin-dependent transitions have different effects on the phase shifts of two circularly polarized lights after being reflected from the optical resonant microcavity. This optical transition process can be characterized by Heisenberg equations for the cavity-field operator \( \hat{a} \) and \( X^- \) dipole operator \( \sigma_- \) in the interaction picture as follows:

\[
\begin{align*}
\frac{d\hat{a}}{dt} &= -[i(\omega_c - \omega) + \frac{\kappa}{2} + \frac{\kappa_s}{2}] \hat{a} - g\sigma_- - \sqrt{\kappa} \hat{a}_{in}, \\
\frac{d\sigma_-}{dt} &= -[i(\omega_X - \omega) + \frac{\gamma}{2}] \sigma_- - g\sigma_\hat{z} \hat{a}, \\
\hat{a}_{out} &= \hat{a}_{in} + \sqrt{\kappa} \hat{a},
\end{align*}
\]

where \( g \) describes the coupling strength of \( X^- \) and the cavity mode. \( \omega_c, \omega \) and \( \omega_X \) describe the frequencies of the cavity mode, the input probe light and the \( X^- \) transition, respectively. \( \gamma/2 \) describes the decay rates of \( X^- \). \( \kappa/2 \) and \( \kappa_s/2 \) describe the decay rates and the side leakage rate of the cavity respectively.

![FIG. 1: The \( X^- \) spin-dependent transitions. (a) A singly charged QD inside a one-side micropillar microcavity with a circular cross section. (b) \( X^- \) spin selection transition rule due to the Pauli’s exclusion principle. L and R describe the left and the right circularly polarized lights, respectively.](image)

Considering the weak excitation condition with \( X^- \) staying in the ground state at most time \((\langle \sigma_z \rangle = 1)\), the reflection coefficient of the QD-cavity system is

\[
r(\omega) = 1 - \frac{\kappa[i(\omega_X - \omega) + \frac{\gamma}{2}]}{[i(\omega_X - \omega) + \frac{\gamma}{2}]^2 + [\frac{\kappa}{2} + \frac{\kappa_s}{2}]^2 + g^2}.
\]

If the \( X^- \) and the cavity mode are uncoupled (a cold cavity), the coupling strength is \( g = 0 \) and the reflection...
coefficient \( r_0(\omega) \) is

\[
 r_0(\omega) = \frac{i(\omega_c - \omega) - \frac{\kappa}{2}}{i(\omega_c - \omega) + \frac{\kappa}{2}}. \tag{3}
\]

Considering \( X^- \)-spin-dependent transitions, the phase shift rules of two circularly polarized lights can be obtained. If the excess electron spin is in the state \(|↑\rangle\), the |\( L \rangle\) light gets a reflection phase shift \( \varphi_h \) with a hot cavity (\( X^- \) and the cavity mode are coupled), and the |\( R \rangle\) light gets a reflection phase shift \( \varphi_0 \) with a cold cavity. If the excess electron spin is in the state \(|↓\rangle\), the |\( L \rangle\) light gets a reflection phase shift \( \varphi_0 \) with a cold cavity, and the |\( R \rangle\) light gets a reflection phase shift \( \varphi_h \) with a hot cavity. If one adjusts the frequencies \( \omega \) and \( \omega_c \), the reflection coefficient can reach \(|r_0(\omega)| \cong 1\) and \(|r_h(\omega)| \cong 1\) in an ideal condition. With the initial states of an electron spin and a circularly polarized light in the superposition states \( \frac{1}{\sqrt{2}}(|↑⟩ + |↓⟩) \) and \( \frac{1}{\sqrt{2}}(|L⟩ + |R⟩) \), the two systems become entangled after the light is reflected by the cavity, that is,

\[
\frac{1}{\sqrt{2}}(|R⟩ + |L⟩) \otimes \frac{1}{\sqrt{2}}(|↑⟩ + |↓⟩) \rightarrow \frac{1}{2}e^{i\varphi_0}(|R⟩ + e^{i\Delta\varphi}|L⟩)|↑⟩ + (e^{-i\Delta\varphi}|R⟩ + |L⟩)|↓⟩, \tag{4}
\]

where \( \Delta\varphi = \varphi_h - \varphi_0 \), \( \varphi_0 = arg[r_0(\omega)] \) and \( \varphi_h = arg[r_h(\omega)] \). \( \theta_F = (\varphi_0 - \varphi_h)/2 = -\theta_F \) is the Faraday rotation angle.

### III. \textbf{BELL-STATE ANALYSIS OF SPATIAL-MODE ENTANGLEMENT}

The photonic spatial Bell-states usually have the form as follows

\[
|ϕ^±⟩_{ab} = \frac{1}{\sqrt{2}}(|a_1b_1⟩ \pm |a_2b_2⟩)_{ab},
\]

\[
|ψ^±⟩_{ab} = \frac{1}{\sqrt{2}}(|a_1b_2⟩ \pm |a_2b_1⟩)_{ab}, \tag{5}
\]

where \( a \) and \( b \) present two photons, and \( a_1 \) (\( b_1 \)) and \( a_2 \) (\( b_2 \)) are the different spatial modes for the photon \( a \) (\( b \)), shown in Fig[2]. The states \( |ϕ^±⟩ \) are always called even-parity states and the states \( |ψ^±⟩ \) are always called odd-parity states.

To distinguish these four Bell states in the spatial-mode DOF, we should first divide the four Bell states into two groups, that is, even-parity states and odd-parity states. This task can be accomplished with a parity-check quantum nondemolition detector (QND). This parity-check QND can be constructed with a one-side QD-cavity system, shown in Fig[2]. Let us assume that the excess electron spin is initially prepared in the state \( \frac{1}{\sqrt{2}}(|↑⟩ + |↓⟩)_c \) and the spatial Bell state of the two-photon system \( ab \) is in the superposition of two circularly polarized components \( (\alpha|R⟩ + \beta|L⟩)_a(\alpha'|R⟩ + \beta'|L⟩)_b \) (here \( |\alpha|^2 + |\beta|^2 = |\alpha'|^2 + |\beta'|^2 = 1 \)). If the frequencies of the input photon and the cavity mode are adjusted as \( \omega - \omega_c \approx \kappa/2 \) to get \( \Delta\varphi = \pi/2 \), after a photon interacts with the QD-cavity twice, the state of the system composed of the input photon and the electron spin becomes

\[
(\alpha|R⟩ + \beta|L⟩)_a \otimes \frac{1}{\sqrt{2}}(|↑⟩ + |↓⟩)_c \rightarrow (\alpha|R⟩ - \beta|L⟩)_a \otimes \frac{1}{\sqrt{2}}(|↑⟩ - |↓⟩)_c. \tag{6}
\]

By measuring the excess electron spin in QD with the orthogonal basis \( \{ |±⟩ = \frac{1}{\sqrt{2}}(|↑⟩ \pm |↓⟩) \} \), one can see that the state of the excess electron spin changes if there is a photon interacting with the QD-cavity system (with a phase-flip operation \( U_p = |R⟩⟨R| - |L⟩⟨L| \) on the photon \( a \), its original state is recovered). If there are two photons interacting with the QD-cavity system, the state of the electron spin becomes unchanged again.

In order to measure the excess electron spin, the orthogonal basis \( \{ |±⟩ \} \) is first rotated to the orthogonal basis \( \{ |↑⟩, |↓⟩ \} \) by applying a Hadamard gate. With an auxiliary photon \( p \), whose original state is \( \frac{1}{\sqrt{2}}(|R⟩ + |L⟩)_p \), put into the cavity, where the photon only interacts with the QD-cavity system once, the state of the system composed of the auxiliary photon and the electron spin in the QD after reflection becomes

\[
\frac{1}{\sqrt{2}}(|R⟩ + |L⟩)_p |↑⟩ \rightarrow \frac{1}{\sqrt{2}}(|R⟩ + i|L⟩)_p |↑⟩, \tag{7}
\]

\[
\frac{1}{\sqrt{2}}(|R⟩ + |L⟩)_p |↓⟩ \rightarrow \frac{1}{\sqrt{2}}(|R⟩ - i|L⟩)_p |↓⟩.
\]

By measuring the state of the output auxiliary photon \( p \) in the orthogonal linear polarizations \( \frac{1}{\sqrt{2}}(|R⟩ \pm i|L⟩) \), one can distinguish whether the state of the excess electron spin in the QD is changed or not. In detail, if the auxiliary photon is in the state \( \frac{1}{\sqrt{2}}(|R⟩ + i|L⟩) \), the state
of the electron spin $e$ does not change. However, if the auxiliary photon is in the state $\frac{1}{\sqrt{2}}(R - iL)$, the state of the electron spin $e$ is changed.

By far, we have constructed a photon-number QND to distinguish an even number of photons from an odd number of photons. If the excess electron spin is changed, there are odd number of photons passing through the QD-cavity system. If the excess electron spin is unchanged, there are an even number of photons passing through the QD-cavity system. In Fig.2 we construct a parity-check QND with this photon number QND. If the state of the excess electron spin in QD is changed, the spatial Bell state input is one of the two odd-parity states $|\psi^{\pm}\rangle$. The input spatial Bell state is one of the two even-parity states $|\phi^{\pm}\rangle$ if the state of the excess electron spin in QD is unchanged.

After dividing the spatial Bell states into an odd-parity states group and an even-parity states group, we have to distinguish the different relative phases in each group. In order to distinguish the Bell state with a relative phase zero from the Bell state with a relative phase $\pi$, Hadamard operations are performed on the two photons with two 50:50 beam splitters (BS) shown in Fig.2. A BS can be used to complete the transformation of photon states in the spatial-mode DOF:

$$
|a_1\rangle \rightarrow \frac{1}{\sqrt{2}}(|c_1\rangle + |c_2\rangle),
$$

$$
|a_2\rangle \rightarrow \frac{1}{\sqrt{2}}(|c_1\rangle - |c_2\rangle),
$$

$$
|b_1\rangle \rightarrow \frac{1}{\sqrt{2}}(|d_1\rangle + |d_2\rangle),
$$

$$
|b_2\rangle \rightarrow \frac{1}{\sqrt{2}}(|d_1\rangle - |d_2\rangle). \tag{8}
$$

The two groups are transformed as follows:

$$
\frac{1}{\sqrt{2}}(|a_1b_1\rangle + |a_2b_2\rangle) \rightarrow \frac{1}{\sqrt{2}}(|c_1d_1\rangle + |c_2d_2\rangle),
$$

$$
\frac{1}{\sqrt{2}}(|a_1b_1\rangle - |a_2b_2\rangle) \rightarrow \frac{1}{\sqrt{2}}(|c_1d_2\rangle + |c_2d_1\rangle),
$$

$$
\frac{1}{\sqrt{2}}(|a_1b_2\rangle + |a_2b_1\rangle) \rightarrow \frac{1}{\sqrt{2}}(|c_1d_2\rangle - |c_2d_1\rangle),
$$

$$
\frac{1}{\sqrt{2}}(|a_1b_2\rangle - |a_2b_1\rangle) \rightarrow \frac{1}{\sqrt{2}}(|c_1d_1\rangle - |c_2d_2\rangle). \tag{9}
$$

This means that the states $|\phi^+\rangle_{ab}$, $|\phi^-\rangle_{ab}$, $|\psi^+\rangle_{ab}$ and $|\psi^-\rangle_{ab}$ will become $|\phi^+\rangle_{cd}$, $|\psi^-\rangle_{cd}$, $|\psi^+\rangle_{cd}$ and $|\psi^-\rangle_{cd}$, respectively. With the four detectors shown in Fig.2 one can completely distinguish the four Bell states in the spatial-mode DOF. If the detectors $c_1$ and $d_1$ or $c_2$ and $d_2$ click, the input state is $|\phi^+\rangle_{ab}$ or $|\psi^+\rangle_{ab}$, respectively. If the detectors $c_1$ and $d_2$ or $c_2$ and $d_1$ click, the input state is $|\phi^-\rangle_{ab}$ or $|\psi^-\rangle_{ab}$, respectively.

Now we have completely distinguish the four spatial-mode Bell states. The relation of the input Bell states and the measurement of the excess electron spin and detectors clicked is shown in Table I. If the excess electron spin in QD is unchanged and the detectors $c_1, d_1$ or $c_2, d_2$ click, the state input is $|\phi^+\rangle$. If the excess electron spin in QD is changed and the detectors $c_1$ and $d_1$ or $c_2$ and $d_2$ click, the input state is $|\psi^-\rangle$. The excess electron spin in QD is unchanged and the detectors $c_1$ and $d_2$ or $c_2$ and $d_1$ click for the input state $|\phi^-\rangle$, and the excess electron spin in QD is changed and the detectors $c_1$ and $d_2$ or $c_2$ and $d_1$ click for the input state $|\psi^-\rangle$.

### IV. ROBUST TWO-STEP QSDC BASED ON SPATIAL ENTANGLEMENT

We will present a robust two-step QSDC protocol, following the ideas in Refs. [38, 39]. With photon pairs in a spatial-mode Bell state, the principle of this robust two-step QSDC can be described in detail as follows.

1. The phase for creating a secure quantum channel between the two users with photon pairs in a spatial-mode Bell state.

In this time, Alice and Bob can create a secure quantum channel with a sequence of photon pairs in a spatial-mode Bell state. In detail, Bob prepares a sequence of photon pairs in which each pair is in the spatial-mode Bell state $|\phi^+\rangle_{ab} = \frac{1}{\sqrt{2}}(|a_1b_1\rangle + |a_2b_2\rangle)_{ab}$. Bob divides the photon pairs into two photon sequences $S_A$ and $S_B$. That is, $S_A$ ($S_B$) is composed of all the photons $a$ ($b$) in the photon pairs, as the same as that in the original two-step protocol [38, 39]. Bob sends the photon sequence $S_A$ to Alice. After Alice receives the sequence $S_A$, she chooses randomly a subset of photon samples from $S_A$ and measures them by choosing randomly one of two nonorthogonal bases for each photon, say $Z$ and $X$. Here $Z = \{|a_1\rangle, |a_2\rangle\}$ and $X \equiv \{|\pm\rangle = \frac{1}{\sqrt{2}}(|a_1\rangle \pm |a_2\rangle\}$. She tells Bob the positions and the outcomes of sampling photons. Bob measures the photons correlated to the samples chosen by Alice with the same bases as those by Alice and then analyzes the security of their quantum channel with a sequence of photon pairs in a spatial-mode Bell state. If Bob confirms that their channel is secure, he tells Alice to encode her secret message on the photons remained in the photon sequence $S_A$. Otherwise, Bob and Alice discard their quantum channel and repeat their quantum communication from the beginning.

In essence, Bob and Alice create a secure quantum channel with a sequence of photon pairs in a spatial-
mode Bell state in the first phase. The eavesdropping check can be accomplished with the correlation between the two photons in each pair, as the same as the Bennett-Brassard-Mermin QKD protocol [4]. More accurately, it is as the same as the eavesdropping check in the original two-step QSDC protocol [38, 39] in principle. However, this process is more robust than that in the original two-step QSDC protocol [38, 39] as the spatial-mode entanglement is more stable than the polarization entanglement of photon pairs, as shown in previous works [61, 67].

(2) The message coding and decoding phase.

After Alice and Bob create a quantum channel securely, they can exchange the secret message directly. That is, Alice encodes her secret message on the photons in the sequence $S_A$ with four unitary operations $U_i$ ($i = 1, 2, 3, 4$) in the spatial-mode DOF. Here

$$U_1 = \left| a_1 \right\rangle \langle a_1 + \left| a_2 \right\rangle \langle a_2 |,$$
$$U_2 = \left| a_1 \right\rangle \langle a_2 + \left| a_2 \right\rangle \langle a_1 |,$$
$$U_3 = \left| a_1 \right\rangle \langle a_1 - \left| a_2 \right\rangle \langle a_2 |,$$
$$U_4 = \left| a_1 \right\rangle \langle a_2 - \left| a_2 \right\rangle \langle a_1 |.$$

(10)

With these unitary operations, Alice can transform the spatial-mode Bell state $|\phi^{+}\rangle_{ab}$ into one of the four Bell states $|\phi^{\pm}\rangle_{ab}$ and $|\psi^{\pm}\rangle_{ab}$.

In order to check eavesdropping, Alice chooses randomly some photons in the sequence $S_A$ as the samples for error rate analysis and she encodes them with the four unitary operations randomly. After coding the message, Alice sends the photon sequence $S_A$ to Bob. By combining the two photon sequences $S_A$ and $S_B$ and performing a BSA on the spatial-mode entangled states of each photon pair, Bob can obtain the information about the unitary operations chosen by Alice in a deterministic way. After filtering out the sample pairs for eavesdropping check, Bob can, in principle, read out the secret message sent by Alice directly if they code the operations $U_1$, $U_2$, $U_3$, and $U_4$ as the message 00, 01, 10, and 11, respectively.

From the description above, one can see that this robust two-step QSDC protocol does not increase the difficulty of its implementation in experiment, compared with the original two-step QSDC protocol [38, 39]. Except for the complete analysis for the four spatial-mode Bell states, all the unitary operations can be accomplished with linear optical elements, such as BSs. However, it improves the robustness of the two-step QSDC protocol largely. Moreover, the present robust two-step QSDC protocol requires Alice to send the photon sequence $S_A$ back to Bob, not the case that Bob sends both the sequences $S_B$ and $S_A$ to Alice, which is different to the original two-step QSDC protocol [38, 39]. This modification can reduce the requirement of entanglement swapping when there is photon loss in the transmission line. Certainly, Alice and Bob should prevent a vicious eavesdropper from stealing their secret message with Trojan horse attack [74, 75].

V. DISCUSSION AND SUMMARY

Bell states analysis is necessary in quantum communication. Many works were focused on a complete and deterministic analysis of Bell states in the polarization DOF of photon pairs with linear optics [70, 71] or nonlinear optics [78]. In 2010, Bonato et al. [33] constructed a complete polarization photonic Bell-state analyzer with double-sided QD-cavity system in weak-coupling regime. In 2011, Hu et al. [36] also constructed a complete polarization photonic Bell-state analyzer using both single-sided and double-sided QD-cavity systems based on GCB. They pointed out that their schemes work with the coherence photon-spin interaction in linear regime. Recently, people find that the spatial-mode entanglement of a photon pair is more robust than its polarization entanglement. This good feature can be used to design some robust quantum communication protocols. In this work, we present a robust two-step QSDC protocol based on the spatial-mode entanglement and the complete BSA. Certainly, this protocol can be used to create a private key between two legitimate users, similar to the works in Refs. [38, 39]. The complete BSA of spatial-mode Bell states in our proposal is also constructed with the GCB of a one-side QD-cavity system working in linear regime. The one-side QD-cavity system is used to construct photon-number QND to distinguish an even number of photons from an odd number of photons which works as parity check gate in spatial-mode BSA. Here an external freedom of electron spin in QD is introduced to assist complete spatial-mode photonic BSA in linear condition.

![FIG. 3: Schematic diagram for the generation of the spatial entanglement from the polarization entanglement of two-photon systems. $a$ and $b$ represent the two photons in a two-photon system whose initial state is $\sqrt{2}(|H\rangle_a|H\rangle_b + |V\rangle_a|V\rangle_b)$. PBS presents a polarizing beam splitter which is used to transmit the photon in the horizontal polarization $|H\rangle$ and reflects the photon in the vertical polarization $|V\rangle$. HWP is a half-wave plate which is used to flip the polarization states of photons, i.e., $|H\rangle \rightarrow |V\rangle$.]

In experiment, the spatial-mode entanglement of a photon pair can be obtained by the transformation from the polarization entanglement. Its principle is shown in Fig.8. That is, one can first produce a photon pair in an entangled state in the polarization DOF $|\phi^{+}_{p}\rangle_{ab} = \sqrt{2}/2(|H\rangle_a|H\rangle_b + |V\rangle_a|V\rangle_b)$ and then transform the polarization entanglement into the spatial entanglement with...
linear optical elements, shown in Fig.8. When the photon pair $ab$ passes through the two PBSs and the two HWP$s$, its state becomes

$$|\Phi^+\rangle_{ab} = |H\rangle_a|H\rangle_b \otimes \frac{1}{\sqrt{2}}(|a_1a|b_1b) + |a_2a|b_2b). \quad (11)$$

This is just the spatial-mode Bell state $|\phi^+\rangle_{ab}$.

In order to construct spatial-mode complete BSA with parity-check gate, the relative phase shift of the left and the right circular polarized lights should be $\Delta \varphi = \pm \pi/2$. This can be achieved by adjusting the frequencies as $\omega_l = \omega_r = \omega_c \approx \kappa/2$ and keeping the cavity side leakage rate as $\kappa_s < 1.3\kappa$. In 2011, Young et al. performed an experiment to measure the quantum-dot-induced phase shift with a quantum dot resonantly coupled to a pillar microcavity ($Q \sim 51000, d = 2.5\mu m$), and showed that a QD-induced phase shift of 0.2 rad between an (effectively) empty cavity and a cavity with a resonantly coupled QD can be deduced by using a single-photon level probe and improving mode matching and pillar design. In an ideal case, the side leakage loss rate $\kappa_s$ is much lower than the cavity loss rate $\kappa$, and the reflection coefficients for the cold and the hot cavities can achieve $|r_0(\omega)| \approx 1$ and $|r_h(\omega)| \approx 1$ for unity fidelity and efficiency. However, in experiment, the side leakage loss of cavity can not be neglected and the fidelity is reduced to $F = |\langle \psi_f | \psi \rangle|^2$. Here $|\psi_f\rangle$ is the final state of the total system which includes the external reservoirs and $|\psi\rangle$ is the ideal state without cavity side leakage. The fidelity and the efficiency of spatial mode BSA process for states $|\psi^\pm\rangle$ are

$$F_1 = \frac{(|r_0|^4 + |r_h|^4 + |r_0|^2|r_h| + |r_0||r_h|^2)^2}{4(|r_0|^2 + |r_h|^2 + |r_0|^2|r_h|^2 + |r_0||r_h|^2)^2},$$

$$\eta_1 = \frac{1}{2}|r_0|^4 + \frac{1}{2}|r_h|^4, \quad (12)$$

and the fidelity and the efficiency of states $|\phi^\pm\rangle$ are

$$F_2 = \frac{(|r_0|^5 + |r_h|^5 + |r_0|^4|r_h| + |r_0||r_h|^4)^2}{8(|r_0|^10 + |r_h|^10 + |r_0|^8|r_h|^2 + |r_0|^2|r_h|^8)^2},$$

$$\eta_2 = \frac{1}{2} + \frac{1}{2}|r_0|^4 + \frac{1}{2}|r_h|^4. \quad (13)$$

From Fig. 4 and Fig. 5, one can see that the fidelity and the efficiency of the even parity states $|\phi^\pm\rangle$ are larger than those of the odd parity states $|\psi^\pm\rangle$. In Fig. 4(a) and Fig. 5(a), the fidelity of the present spatial-mode BSA is relatively high in both the strong coupling regime ($g > \kappa + \kappa_s/4$) and the weak coupling regime ($g < \kappa + \kappa_s/4$). In Fig. 4(b) and Fig. 5(b), the high efficiency of the present spatial-mode BSA can only be gotten in the strong coupling regime. That is, our BSA proposal works efficiently in the strong coupling regime, which is challenging to be observed in various QD-cavity systems. The strong coupling strength $g \approx 0.5(\kappa + \kappa_s)$ was observed in $d = 1.5\mu m$ micropillar microcavities with the quality factor $Q = 8800$, and this coupling strength can be increased to be $g \approx 2.4(\kappa + \kappa_s)$ ($Q \sim 40000$) by improving the sample designs, growth, and fabrication [82]. For the odd-parity states $|\psi^\pm\rangle$, if the coupling strength is $g \approx 2.4(\kappa + \kappa_s)$, the fidelity and the efficiency are $F_1 = 99.99\%$ and $\eta_1 = 98.1\%$ with $\kappa_s/\kappa = 0$, and $F_1 = 69.6\%$ and $\eta_1 = 53.2\%$ with $\kappa_s/\kappa = 0.7$. Both the fidelity and the efficiency are high with the strong coupling strength, but they are largely reduced by the side leakage and cavity loss rate. In experiment, the quality factor is dominated by the side leakage and cavity loss rate of micropillar rather than the output coupling rate. In Ref. [36], Hu et al. reduced the side leakage and cavity loss rate to $\kappa_s/\kappa \sim 0.7$ with the coupling strength $g \approx \kappa + \kappa_s$ ($Q \sim 17000$) by thinning down the top mirrors of high-Q micropillar ($d = 1.5\mu m$). In this case, the fidelity and the efficiency of states $|\psi^\pm\rangle$ is $F_1 = 71.3\%$ and $\eta_1 = 47.8\%$. The higher the fidelity and the efficiency are demanded, the smaller $\kappa_s/\kappa$ are required. This is quite a challenging for micropillar microcavities, because the strong coupling was achieved in a large micropillar ($d = 7.3\mu m$) with a large side leakage in recent experiments.

Besides micropillar microcavities, there are many other factors which affect the fidelity of our BSA proposal. The spin decoherence is the one we should consider with the fidelity decoherence factor $F^\prime = [1 + \exp(-\Delta t/T^*_S)]/2$. Here $T^*_S$ is the electron spin decoherence time and $\Delta t$ is the time interval between two input photons. As $T^*_S$ could be extended to $\mu s$ with spin echo techniques, which is longer than $\Delta t$ (ns) in the weak excitation approximation, this fidelity decoherence factor can be neglected. The optical dephasing time of exciton, which is ten times longer than cavity photon lifetime [34, 86], also reduces the fidelity by a few percent. While the hole spin in $X^−$ (absence of significant hyperfine interaction) is three orders longer than the cavity photon life time [37, 87], and the spin dephasing of $X^−$ can be safely neglected. The hole mixing can also reduce the fidelity due
to unperfect optical selection rule \[90\]. For charged exciton $X^-$, this effect can be neglected by the quenched exchange interaction \[91\] \[92\].

In summary, we have presented a complete and deterministic protocol for the BSA in the spatial-mode DOF of a photon pair, resorting to the GCB based on a quantum microcavity. The whole process for BSA is divided into two parts. First, one divides the four Bell states in spatial-mode DOF into two groups, that is, the even-parity group and the odd-parity group, according to their parities of the two photons with a parity-check QND based on QD-cavity system. Subsequently, one can distinguish the relative phase of the two states in each group by transforming the difference of the phases into that of the spatial modes with BSs and QND. As the spatial entanglement of two-photon systems is more robust than the polarization entanglement, we presented a robust two-step quantum secure direct communication protocol with the spatial-mode Bell states and their BSA. With current technology, our BSA proposal for spatial-mode Bell states works in both the strong coupling regime ($g > (\kappa + \kappa_s)/4$) and the weak coupling regime ($g < (\kappa + \kappa_s)/4$) if the side leakage and cavity loss rate is small. Maybe this BSA proposal for spatial-mode Bell states is very useful in the applications in robust quantum communication protocols, such as QKD, QSS, quantum state sharing, deterministic secure quantum communication, and so on.

This work is supported by the National Natural Science Foundation of China under Grant Nos. 10974020 and 11174039, NCET-11-0031, and the Fundamental Research Funds for the Central Universities.

\[1\] M.A. Nielsen, I.L. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, Cambridge, UK, 2000)
\[2\] R. Horodecki, P. Horodecki, M. Horodecki, K. Horodecki, Rev. Mod. Phys. **81**, 865 (2009)
\[3\] A.K. Ekert, Phys. Rev. Lett. **67**, 661 (1991)
\[4\] C.H. Bennett, G. Brassard, N.D. Mermin, Phys. Rev. Lett. **68**, 557 (1992)
\[5\] N. Gisin, G. Ribordy, W. Tittel, H. Zbinden, Rev. Mod. Phys. **74**, 145 (2002)
\[6\] F.G. Deng, G.L. Long, Phys. Rev. A **68**, 042315 (2003)
\[7\] X.H. Li, F.G. Deng, H.Y. Zhou, Phys. Rev. A **78**, 022321 (2008)
\[8\] C.H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, W.K. Wootters, Phys. Rev. Lett. **70**, 1895 (1993)
\[9\] M. Żukowski, A. Zeilinger, M.A. Horne, A.K. Ekert, Phys. Rev. Lett. **71**, 4287 (1993)
\[10\] C.H. Bennett, S.J. Wiesner, Phys. Rev. Lett. **69**, 2881 (1992)
\[11\] X.S. Liu, G.L. Long, D.M. Tong, F. Li, Phys. Rev. A **65**, 022304 (2002)
\[12\] M. Hillery, V. Bužek, A. Berthiaume, Phys. Rev. A **59**, 1829 (1999)
\[13\] A. Karlsson, M. Koashi, N. Imoto, Phys. Rev. A **59**, 162 (1999)
\[14\] L. Xiao, G.L. Long, F.G. Deng, J.W. Pan, Phys. Rev. A **69**, 052307 (2004)
\[15\] A.M. Lance, T. Symul, W.P. Bowen, B.C. Sanders, P.K. Lam, Phys. Rev. Lett. **92**, 177903 (2004)
\[16\] F.G. Deng, C.Y. Li, Y.S. Li, H.Y. Zhou, Y. Wang, Phys. Rev. A **72**, 022338 (2005)
\[17\] F.G. Deng et al., Phys. Rev. A **72**, 044301 (2005); F.G. Deng et al., Eur. Phys. J. D **39**, 459 (2006)
\[18\] X.H. Li et al., J. Phys. B **39**, 1975 (2006)
\[19\] Z.X. Man, Y.J. Xia, N.B. An, Eur. Phys. J. D **42**, 333 (2007); Z.Y. Wang, H. Yuan, S.H. Shi, Z.J. Zhang, Eur. Phys. J. D **41**, 371 (2007)
\[20\] X.H. Li, B.K. Zhao, Y.B. Sheng, F.G. Deng, H.Y. Zhou, Int. J. Quantum Inform. **7**, 1479 (2009)
\[21\] L. Vaidman, N. Yoran, Phys. Rev. A **59**, 116 (1999)
\[22\] N. Lütkenhaus, J. Calsamiglia, K.A. Suominen, Phys. Rev. A **59**, 3295 (1999)
\[23\] J. Calsamiglia, Phys. Rev. A **65**, 030301(R) (2002)
\[24\] K. Mattle, H. Weinfurter, P.G. Kwiat, A. Zeilinger, Phys. Rev. Lett. **76**, 4656 (1996)
\[25\] J.A.W. van Houwelingen, N. Brunner, A. Beveratos, H. Zbinden, N. Gisin, Phys. Rev. Lett. **96**, 130502 (2006)
\[26\] R. Ursin, T. Jennewein, M. Aspelmeyer, R. Kaltenbaek, M. Lindenthal, P. Walther, A. Zeilinger, Nature (London) **430**, 849 (2004)
\[27\] P.G. Kwiat, H. Weinfurter, Phys. Rev. A **58**, 2623(R) (1998)
\[28\] S.P. Walborn, S. Padua, C.H. Monken, Phys. Rev. A **68**, 042313 (2003)
\[29\] C. Schuck, G. Huber, C. Kurtsiefer, H. Weinfurter, Phys. Rev. Lett. **96**, 190501 (2006); M. Barbieri, G. Vallone, P. Mataloni, F. De Martini, Phys. Rev. A **75**, 042317 (2007)
\[30\] J.T. Barreiro, T.C. Wei, P.G. Kwiat, Nature Phys. **4**, 282 (2008); T.C. Wei, J.T. Barreiro, P.G. Kwiat, Phys. Rev. A **75**, 060305(R) (2007)
\[31\] T. Calarco, A. Datta, P. Fedichev, E. Pazy, P. Zoller, Phys. Rev. A **68**, 012310 (2003)
\[32\] C.Y. Hu, A. Young, J.L. O’Brien, W.J. Munro, J.G. Rarity, Phys. Rev. B **78**, 085307 (2008)
V1 [the first version announced on 13 Dec 2000 in arXiv:quant-ph/0012056 and it claims clearly that this protocol can be used to transmit secret message directly. Its simplified version is published in Phys. Rev. A 65, 032302 (2002)]

V. Loo, L. Lanco, A. Lemaître, I. Sagnes, O. Krebs, P. Senellart, Appl. Phys. Lett. 87, 161306(R) (2003)