Entanglement preparation and quantum communication with atoms in optical cavities

Peng Xue,* Chao Han, Bo Yu, Xiu-Min Lin, and Guang-Can Guo†

Key Laboratory of Quantum Information, University of Science and Technology of China, Hefei 230026, People's of Republic of China

(Received 8 July 2003; published 17 May 2004)

We propose an experimentally feasible scheme to generate general entangled states between atoms in spatially separate cavities, and then show one of the applications—a secure communication allowing asymptotically key distribution and quasisecure direct communication. The scheme involves laser manipulation of atoms in a high-Q cavity, adjustable quarter- and half-wave plates, beam splitter, polarizing beam splitters, and single-photon detectors, and well fits the status of the current experimental technology.

DOI: 10.1103/PhysRevA.69.052318 PACS number(s): 03.67.Hk, 03.65.Ud, 42.50.Gy

I. INTRODUCTION

Over the last decade there has been much activity in the theoretical [1,2] and experimental [3] study of simple nontrivial models of quantum-optical interactions involving one atom with a few energy levels and one or more near resonant modes of the quantized electromagnetic field. Recently, trapping of single atoms in high-Q cavities opens up exciting possibilities which have wide applications such as for generation of nonclassical or entangled optical pulses [4,5], for observing strong cavity-QED effects [6–8], and more remarkably, for implementation of quantum communication and computation [9–13]. The trapping potential for confining single atoms can be created by diverse avenues, including the cavity-QED light itself [6,7], by additional far-off-resonant trapping beams [14], and by combining single trapping atoms with high-Q cavities [15,16]. Remarkably, cavity QED, where atoms interact with a quantized electromagnetic field, has already proven to be an ideal system for generating entangled state [17]. Very recently, some schemes with inherent robustness to diverse sources of noise have been proposed for entangling atoms in one cavity [18–22] as well as in spatiality separate cavities [23,24]. The protocols are thereby probabilistic, succeeding only conditionally for particular measurement results. Imperfections and noise in these schemes decrease the success probability, but have no influence on the fidelity of the intended state generation for the "successful"subset of trials.

In the paper, we would like to propose a scheme for the preparation of general entanglement between atoms in different cavities. We consider a system consisting of a single five-level atom, located inside an external driven optical cavity. The atom interacts with environment via a partially transparent mirror. The output field from the cavities monitored using the single-photon detectors. Our scheme involves the passage of an atom with Zeeman substructure through overlapping cavity and laser fields, and is based on the adiabatic transfer of atomic ground-state Zeeman coherence to the cavity mode. Compared with the previous scheme, our protocol has the following favorable features: (1) It is much more efficient in the sense that the success probability can be close to 1 in the ideal case; (2) it is more insensitive to certain practical sources of noise, such as randomness in the atom's position, atomic spontaneous emission, or detection inefficiency, which only decrease the success probabilities, but have no influence on the fidelity of the intended state generation for the successful subset of trials; (3) individual addressing of atoms is not required, nor are single-photon states as initial resources.

This paper is organized as follows: in the following section, we explain the basic idea of the method in the ideal case where no dissipation takes places, and then describe and solve the model Hamiltonian analytically following some well-known approach based on the adiabatic approximation. In Sec. III, the scheme is analyzed in the more realistic situation. We propose a protocol that allows the generation of a maximally entangled state between individual atoms held in spatially separate cavities. Two Raman interactions are used to entangle the electronic levels and the quantized cavity field in each atom-cavity system. The output fields of the two cavities are superimposed and detected by single-photon detectors. In Sec. IV, by making use of quantum memory available in atomic internal levels, the "EPR" states can be put into many applications, for example, secure direct communication allowing asymptotically secure key distribution and quasisecure direct communication, and in the latter case, the communication protocol is quasisecure, i.e., an eavesdropper is able to gain a small amount of message information before being detected. In case of a key distribution, the protocol is asymptotically secure. In contrast to other quantum cryptographic schemes, the presented scheme is instantaneous, that is, the information can be decoded during the transmission. This improvement is obtained via random switching between two distinct communication modes—a transmission mode and detection mode. The key (or plain text) is generated (or transmitted) in the transmission mode, while the eavesdropping is detected in the other mode. The only parameter which has to be analyzed in order to detect the eavesdropper is the correlation of bits generated in the detection mode. The basic idea of the protocol has been raised by Boström *et al.* [25]. In the last section, we summarize our proposal, and discuss how some states are more robust than other ones against dissipation and loss. The derivation of the evolution in the presence of dissipation uses the standard method of adiabatic elimination and produces quite complicated equations.

*Email address: xuepeng@mail.ustc.edu.cn

†Email address: gcguo@ustc.edu.cn

II. CAVITY QED WITH A TRAPPING ATOM IN AN IDEAL CASE

First we explain the basic idea of this method by considering a single trapping atom, with relevant level configuration shown as Fig. 1. We consider a double-Λ-type five-level configuration of atomic state of ^{87}Rb by way of example. In this case, $|g\rangle$, $|h\rangle$, and $|v\rangle$ with energy differences ω_{gh} and ω_{gv} of the simplified five-level modes can be achieved in pairs of Zeeman sublevels of electronic ground-state $(5S_{1/2})$ ^{87}Rb atoms, corresponding respectively, to $|F=1,M_F=0\rangle$, $|F=2,M_F=-2\rangle$, and $|F=2,M_F=2\rangle$, with magnetic quantum numbers differing by 2. The upper levels $|e_h\rangle$ and $|e_v\rangle$ with energy splittings ω_{ge_h} and ω_{ge_v} to the ground state $|g\rangle$ $(\hbar=1)$ are the Zeeman sublevels of electronic excited $5P_{1/2}$ state, corresponding to $|F=2,M_F=-1\rangle$ and $|F=2,M_F=1\rangle$, respectively. The two pairs of Zeeman sublevels of the ground states $|g\rangle,|h\rangle$ and $|g\rangle,|v\rangle$ are coupled via two far-detuned Raman transition, i.e., all fields have the same large detuning Δ on their respective transitions to the upper levels $|e_h\rangle$ and $|e_v\rangle$. The transitions $|e_s\rangle\rightarrow|s\rangle$ (here $s=h,v$) are coupled resonantly to the cavity-QED mode $\hat{c}_s$ with the coupling rates $g_s(\mathbf{r},t)$ which depends on the atom's position $\mathbf{r}$ and the time of the atom across the cavity field profile, and can be factorized as

$$g_s(\mathbf{r},t)=g_0^s(t)\chi(\mathbf{r}). \tag{1}$$

We assume for simplicity that $\hat{c}_h$ and $\hat{c}_v$ have the same spatial mode structure with the same frequency ω_o (for example, they can be of different polarizations). Two classical lasers with the same frequency ω_l and different polarizations couple to the transitions $|g\rangle\rightarrow|e_s\rangle$ with the Rabi frequencies $\Omega_s(\mathbf{r},t)$, through other cavity modes $\hat{c}_s'$. The two lasers are far-off-resonant to the cavity modes $\hat{c}_s$ with a large detuning ω_{gs} denoting the splitting between the levels $|g\rangle$ and $|s\rangle$. For simplicity, we assume that $\hat{c}_s$ and $\hat{c}_s'$ have the same spatial mode structure with the same frequency and different polarizations. Then the Rabi frequency will depend on the atom's position $\mathbf{r}$ by the same mode function $\chi(\mathbf{r})$, i.e., $\Omega_s(\mathbf{r},t)$ can be factorized as

$$\Omega_s(\mathbf{r},t)=\Omega_0^s(t)\chi(\mathbf{r}). \tag{2}$$

The density matrix ρ of this system satisfies the equation

$$\frac{d\rho}{dt}=-i[H_{eff},\rho], \tag{3}$$

and the effective Hamiltonian H_{eff} is given by

$$H_{eff}=-\sum_{s=h,v}\left[\frac{|\Omega_s(\mathbf{r},t)|^2}{4}|g\rangle\langle g|+|g_s(\mathbf{r},t)|^2\hat{c}_s^\dagger\hat{c}_s|s\rangle\langle s| + \left(\frac{\Omega_s(\mathbf{r},t)g_s^*(\mathbf{r},t)}{2}\hat{c}_s^\dagger|s\rangle\langle g|+\text{H.c.}\right)\right]. \tag{4}$$

Here we adiabatically eliminate the excited state of the atom by assuming that the population of that state is negligible.

The effective Hamiltonian $H_{eff}(t)$ has the property that it couples only state within the family, or manifold, $\{|g,n\rangle,|h,n+1\rangle,|v,n+1\rangle\}$ where $|n\rangle$ represents an n-photon Fock state of the cavity mode. The adiabatic energy eigenvalues of the Hamiltonian associated with a particular family of states are

$$E_1=n\omega_o, \tag{5}$$

$$E_2=n\omega_o+\frac{g^2(\mathbf{r},t)(n+1)}{\Delta},$$

$$E_3=n\omega_o+\frac{2g^2(\mathbf{r},t)(n+1)+\Omega^2(\mathbf{r},t)}{2\Delta}.$$

For simplicity, we assume that the Rabi frequencies and the coupling coefficients are real and satisfy $g_h(\mathbf{r},t)=g_v(\mathbf{r},t)=g(\mathbf{r},t)$, and $\Omega_h(\mathbf{r},t)=\Omega_v(\mathbf{r},t)=\Omega(\mathbf{r},t)$. Of particular interest to us is the eigenstate corresponding to $E_1=n\omega_o$ which is given by

$$|E_n\rangle=\frac{2g_0(t)\sqrt{n+1}|g,n\rangle-\Omega_0(t)(|h,n+1\rangle+|v,n+1\rangle)}{\sqrt{4g_0^2(t)(n+1)+2\Omega_0^2(t)}}. \tag{6}$$

This eigenstate does not contain any contribution from the excited state (hence the term "dark" state), and is independent of the detuning Δ. The possibility for adiabatic passage arises from the following behavior of $|E_n\rangle$:

$$|E_n\rangle\rightarrow|g,n\rangle \quad \text{for } \Omega_0(t)/g_0(t)\rightarrow 0, \tag{7}$$

$$|E_n\rangle\rightarrow|h,n+1\rangle \quad \text{or} \quad |v,n+1\rangle \quad \text{for } g_0(t)/\Omega_0(t)\rightarrow 0,$$

that is, for the pulse sequence in which the $\Omega_0(t)$ pulse is time delayed with respect to $g_0(t)$, the state $|g,n\rangle$ may be adiabatically transformed into the state $|h,n+1\rangle$ or $|v,n+1\rangle$ with the same probability.

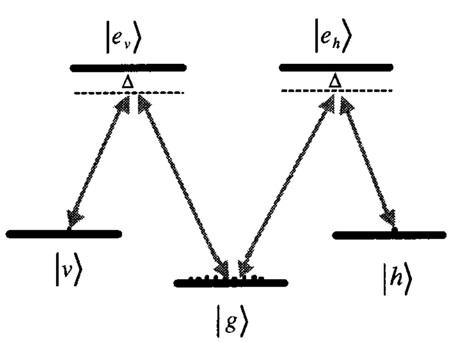

FIG. 1. The relevant-type double-Λ-level structure of the alkali atoms in the ensembles. The metastable lower states $|g\rangle$, $|h\rangle$, and $|v\rangle$ can be achieved by, for example, Zeeman sublevels of electronic ground states $5S_{1/2}$ ^{87}Rb atoms, and $|e_h\rangle$ and $|e_v\rangle$ $(5P_{1/2})$ are the excited states.

III. ANALYSIS INCLUDING DISSIPATION AND NOISE

The main purpose of this paper is to demonstrate that it is possible to use two different cavities to entangle atoms even in situations where substantial dissipation is present. In this section, we analyze the performance of our proposal in the presence of the two main decoherence mechanisms, spontaneous emission and cavity decay.

The full master equation for the density operator ρ then takes the form

$$\frac{d\rho}{dt} = -i[H',\rho] + \hat{J}_1\rho\hat{J}_1^\dagger + \hat{J}_2\rho\hat{J}_2^\dagger + \hat{J}_3\rho\hat{J}_3^\dagger + \hat{J}_c\rho\hat{J}_c^\dagger, \qquad (8)$$

where we have defined the effective non-Hermitian Hamiltonian (here, we have adiabatically eliminated the upper levels $|e_h\rangle$ and $|e_v\rangle$)

$$H' = -\sum_{s=h,v}\left\{\frac{\Delta + i\Gamma/2}{\Delta^2+\Gamma^2/4}\left[\frac{\Omega^2(\mathbf{r},t)}{2}|g\rangle\langle g| + g^2(\mathbf{r},t)\hat{c}_s^\dagger\hat{c}_s|s\rangle\langle s| + \left(\frac{\Omega(\mathbf{r},t)g(\mathbf{r},t)}{2}\hat{c}_s^\dagger|s\rangle\langle g| + \text{H.c.}\right)\right] + \frac{i}{2}\kappa_s\hat{c}_s^\dagger\hat{c}_s\right\}. \qquad (9)$$

The excited state $|e_h\rangle$ (or $|e_v\rangle$) is assumed to have three independent decay channels: each of them may decay to their two lower states $|g\rangle$ and $|h\rangle$ (or $|g\rangle$ and $|v\rangle$) with decay rates γ_1 and γ_2, respectively, and it may decay to some other states $|o\rangle$ with a decay rate γ_3. And Γ is the total decay rate of the excited states $\Gamma=\gamma_1+\gamma_2+\gamma_3$. The total effect of the spontaneous emission is described by three relaxation operators

$$\hat{J}_1 = \frac{\sqrt{\gamma_1}}{\Delta - i\Gamma/2}[g(\mathbf{r},t)(\hat{c}_v|g\rangle\langle v| + \hat{c}_h|g\rangle\langle h|) + \Omega(\mathbf{r},t)|g\rangle\langle g|], \qquad (10)$$

$$\hat{J}_2 = \frac{\sqrt{\gamma_2}}{\Delta - i\Gamma/2}\left[g(\mathbf{r},t)(\hat{c}_v|v\rangle\langle v| + \hat{c}_h|h\rangle\langle h|) + \frac{\Omega(\mathbf{r},t)}{2}(|v\rangle\langle g| + |h\rangle\langle g|)\right],$$

$$\hat{J}_3 = \frac{\sqrt{\gamma_3}}{\Delta - i\Gamma/2}[g(\mathbf{r},t)(\hat{c}_v|o\rangle\langle v| + \hat{c}_h|o\rangle\langle h|) + \Omega(\mathbf{r},t)|o\rangle\langle o|].$$

To describe the decay of the cavity with the rates κ_h and κ_v, we introduce a relaxation operator

$$\hat{J}_c = \sqrt{\kappa_h}\hat{c}_h + \sqrt{\kappa_v}\hat{c}_v. \qquad (11)$$

The interaction Hamiltonian in the rotating frame is

$$H_{int} = -\sum_{s=h,v}\left[\frac{\Delta + i\Gamma/2}{2\Delta^2+\Gamma^2/2}\Omega(\mathbf{r},t)g(\mathbf{r},t) \times(\hat{c}_s^\dagger|s\rangle\langle g| + \text{H.c.}) + \frac{i}{2}\kappa_s\hat{c}_s^\dagger\hat{c}_s\right]. \qquad (12)$$

We then adiabatically eliminate the cavity in the Heisenberg picture by assuming the "bad cavity" limit $\kappa_s \gg \Omega(\mathbf{r},t)g(\mathbf{r},t)\Delta/(\Delta^2+\Gamma^2/4)$. Setting $d\hat{c}_s/dt=-i[\hat{c}_s,H_{int}]=0$ we obtain

$$\hat{c}_s = -\frac{2\Omega(\mathbf{r},t)g(\mathbf{r},t)}{i\kappa_s(\Delta - i\Gamma/2)}|s\rangle\langle g| + \text{noise}, \qquad (13)$$

where the noise ensures the communication relation of the operator. The cavity output $\hat{c}_{out}^s(t)$ is connected with the cavity modes $\hat{c}_s$ through the standard input-output relation $\hat{c}_{out}^s(t)=\hat{c}_{in}^s(t)+\sqrt{\kappa_s}\hat{c}_s$, where $\hat{c}_{in}^s(t)$ is the input vacuum field with the property $[\hat{c}_{in}^s(t),\hat{c}_{in}^{s\dagger}(t')]=\delta(t-t')$.

We are interested in the limit for which the variation rate of $\Omega_0(t)$ is significantly smaller than the cavity decay rates κ_h and κ_v. In this limit, we can define an effective single-mode bosonic operator $\hat{c}_{eff}^s$ (here $s=h,v$) from the cavity output operator $\hat{c}_{out}^s(t)$ as $\hat{c}_{eff}^s=\int_0^T f_s(t)\hat{c}_{out}^s(t)dt$, where T is the pulse duration and $f_s(t)$ is the output pulse shape, which is determined by the shape of $\Omega_0(t)$ as $f_s(t) =\sqrt{\kappa_s}\sin\,\theta(t)\exp[-(\kappa_s/2)\int_0^t \sin^2\theta(\tau)d\tau]$ with $\sin\,\theta(t) =\Omega_0(t)/\sqrt{2g_0^2(t)+\Omega_0^2(t)}$.

The atom in each cavity is initially prepared in the ground state $|g\rangle$, but the basis vectors of a qubit are represented by the states $|h\rangle$ and $|v\rangle$. The cavity mode is put in the vacuum state. The atom in each cavity is illuminated by the two driving lasers with the same frequency and different polarizations (σ_+ and σ_-), and transferred with the probability $p_c\approx 1$ to the metastable states $|h\rangle$ and $|v\rangle$ by emitting a photon from the transitions $|e_h\rangle\to|h\rangle$ and $|e_v\rangle\to|v\rangle$, and the final state between the atom and the corresponding cavity output will quickly approach the form

$$|\varphi\rangle_\lambda = (|h\rangle|H\rangle_c + |v\rangle|V\rangle_c)/\sqrt{2}, \qquad (14)$$

where $\lambda=1,2$. Here, H and V, respectively, represent the right (σ_+) and left (σ_-) circular polarization which can be turned into horizontal and vertical polarizations of a photon by a quarter-wave plate (QWP). In the following, $|H\rangle_c$ and $|V\rangle_c$ represent the photon states with the horizontal and vertical polarizations, respectively. If the two driving pulses have the same shape $\Omega(\mathbf{r},t)$ for the two cavities, the output single-photon pulses from the two cavities will also have the same shape $f_s(t)$ and they will interfere with high visibility at the polarizing beam splitter (PBS). If one gets a "click" from each of the detectors at the outputs of the PBS, the two incoming photons can both be either in $|H\rangle_c$ or $|V\rangle_c$, and the possibility amplitudes are coherently superposed when the incoming photon pulses overlap with each other with the same shape. Therefore, the measurement in Fig. 2, together with the half-wave plate (HWP), corresponds to projecting the whole state $|\varphi\rangle_1\otimes|\varphi\rangle_2$ between the atoms and photons onto a subspace with the projection operator given by $P =|HV\rangle_c\langle HV|+|VH\rangle_c\langle VH|$. Within this measurement scheme, the state $|\varphi\rangle_1\otimes|\varphi\rangle_2$ is effectively equivalent to the state

$$|\varphi_{eff}\rangle \propto P|\varphi\rangle_1\otimes|\varphi\rangle_2 \propto (|hv\rangle\otimes|HV\rangle_c + |vh\rangle\otimes|VH\rangle_c)/\sqrt{2}. \qquad (15)$$

The 45° polarizer projects the photon polarizations from the $\{|H\rangle_c,|V\rangle_c\}$ basis to $\{(|H\rangle+|V\rangle)_c/\sqrt{2},(|H\rangle-|V\rangle)_c/\sqrt{2}\}$. After the measurement, the two atoms will be prepared in EPR state $|\Psi^+\rangle_a=(|hv\rangle+|vh\rangle)/\sqrt{2}$. The polarizer can also be replaced by HWP and PBS with both of its output

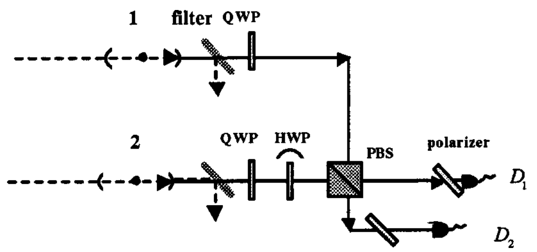

FIG. 2. We consider a setup in which individual atoms are trapped inside two spatially separated optical cavities 1 and 2. The atoms are illuminated by the synchronized pumping laser pulses and the forward-scattering Stokes pulses can leak out the cavities and are collected in the beam splitter after the filters. The dashed line represents the pumping laser pulses with the frequency ω_l and the solid line represents the Stokes pulses.

detected by single-photon detectors. The overall success probability of this scheme becomes $p=1/2$. Before introducing the applications of the EPR state, we offer a few remarks about this two-cavity scheme. First, it is evident that the scheme is inherently robust to atomic spontaneous emission, output coupling inefficiency, and detector inefficiency, all of which contribute to loss of photon. Since a click from each of the detectors D_1 and D_2 is never recorded if one photon is lost, these processes simply decrease the success probability p by a factor of η^2 (where $1-\eta$ denotes the loss for each of the photons), but have no influence on the fidelity of the final state. Second, our scheme does not require localization of the atom in the cavity to the Lamb-Dick limit. For the standing-wave cavity and with the collinear pumping configuration proposed in Ref. [23], $\Omega(\mathbf{r},t)$ and $g(\mathbf{r},t)$ depend on the atom's position through approximately the same cavity mode function. The pulse shapes $f_h(t)$ and $f_v(t)$, which are determined by ratio $\Omega_0(t)/g_0(t)$, thus become basically independent of the random variation in the same cavity mode function. For a traveling-wave cavity or for a free-space configuration, the atom's position only affects the common phase of the coupling rate $g(\mathbf{r},t)$ and in the case, a transverse pumping configuration also suffices since the randomness in the common phase of $g(\mathbf{r},t)$ has no influence on the final entangled state.

IV. THE EXPERIMENTAL REALIZATION OF SECURE DIRECT COMMUNICATION

After the maximally entangled state has been established between two distant sites, we would like to use it in one of the communication protocols, for example secure direct communication, which is achieved with the setup shown in Fig. 3. There are two users, Alice and Bob, who are connected by a quantum channel and a classical public channel. The quantum channel consists usually of an optical fiber. The public channel, however, can be any communication link. Suppose that Bob wants to communicate N-bit message $m^N=(m_1,\ldots,m_N)$ to Alice. Each of them has a set of atoms trapping in optical cavities. Let us give an explicit algorithm for the protocol.

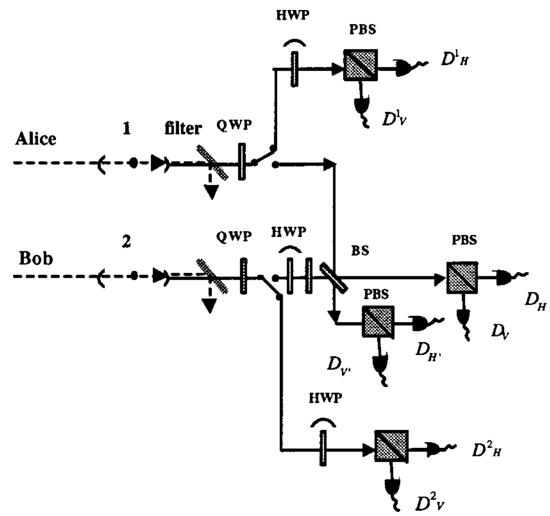

FIG. 3. Schematic setup for the realization of the secure direct communication between two users. In each station, there is a device called "space optical switch" which causes the photons to be sent to the proper mode via fiber. The dashed line represents the repumping laser pulses with the frequency ω_o and the solid line represents the forward-scattering Stokes pulses.

Step 1. Initially, they prepare N pairs of atoms in the different cavities in the maximally entangled state $|\Psi^+\rangle_a$ following the way proposed above.

Step 2. The atoms of each pair belonging to Alice are considered as home qubits, while the other ones belonging to Bob are travel qubits.

Step 3. There are two different repumping pulsed lasers with the same transition frequency $\omega_{repump}=\omega_o$ and different polarizations (σ_+ and σ_-), which induce Raman transitions $|h\rangle \leftrightarrow |g\rangle$ and $|v\rangle \leftrightarrow |g\rangle$, respectively. We are particularly interested in the forward-scattering Stokes light from the two Raman transitions. The two users apply both laser pulses synchronously to measure their atoms. It can be achieved by a Hadamard transformation using a beam splitter (BS). The excitations in the modes $|h\rangle$ and $|v\rangle$ can be transferred to optical excitations (i.e., the forward-scattering Stokes light), which can be used in the secure direct communication. In fact, we use the polarization degree of freedom of the photons from optical excitations. The effective state of the photons after the QWPs which turn the Stokes light to linearly polarized photon is

$$|\Psi^+\rangle_c = (|HV\rangle + |VH\rangle)_c/\sqrt{2}. \tag{16}$$

When two photons are maximally entangled in their polarization degree of freedom, each single photon is not polarized at all. One bit of information can be encoded in the state $|\Psi^+\rangle_c$, which is completely unavailable to anyone who has only access to one of the photons. For each user, there are two modes, the detection mode to detect any eavesdropper, and the transmission mode to transmit the message from Bob to Alice.

Step 4. With a probability λ_d, Bob switches to the detection mode and proceeds with step (d1); else, he starts with step (t1) (the transmission mode).

TABLE I. Overview of possible manipulations and detection events of the transmission mode in secure direct communication with the correlated photons.

m_n	Bob's operator	HWP	QWP	State sent	Alice's registration events
0	I	0°	0°	$\vert\Psi^+\rangle_c$	coinc. between D_H and D_V or $D_{H'}$ and $D_{V'}$
1	σ_z	0°	90°	$\vert\Psi^-\rangle_c$	coinc. between D_H and $D_{V'}$ or $D_{H'}$ and D_V

A. The detection mode

The detection modes are the following.

(d1): For each photon from the optical excitation, Bob has two types of measurements B_i. One measurement is along rectilinear basis (i.e., $B_0=\{|H\rangle_c,|V\rangle_c\}$), and the other is along diagonal basis [i.e., $B_1=\{(1/\sqrt{2})(|H\rangle+|V\rangle)_c,(1/\sqrt{2})(|H\rangle-|V\rangle)_c\}$]. He chooses between the two types at random, which can be achieved by a HWP and PBS. If he detects his photon in the state $|H\rangle_c$ or $(1/\sqrt{2})(|H\rangle+|V\rangle)_c$ (i.e., the detector D_H^2 is fired), he obtains the value $j=0$; else, the measurement yields the result $j=1$, and potentially reveals one bit of information. He writes down his measurement bases and the results of the measurements.

(d2): He sends the two bits i and j through the public channel to Alice.

(d3): When Alice receives the two bits, she switches to the detection mode and measures her photon from the optical excitation in the same basis B_i resulting in the value k [26].

(d4): For the perfect anticorrelation of the state $|\Psi^+\rangle_c$, if j equals k, Eve is detected, and they abort the protocol; else, they go to Step 3.

B. The transmission mode

The transmission modes are the following.

(t1): For one bit of message m_n, Bob encodes the message on his photon from the optical excitation. If $m_n=0$, Bob applies the coding operation—single-bit rotation σ_z on his photon, else, if $m_n=1$, he does nothing, i.e., performs the operator I. And then he sends it back to Alice's Bell-state analyzer. For polarization encoding, the necessary transformations of Bob's photon from the optical excitation are performed by rotating the optic axis of the first QWP to turn the Stokes light to linearly polarized photon, and using a HWP for changing the polarization and the second QWP to generate the polarization-dependent phase shift. The component polarized along the axis of the second QWP is advanced by $\pi/2$ relative to the other. Reorienting the optical axis from vertical to horizontal causes a net phase change of π between $|H\rangle_c$ and $|V\rangle_c$. The photon manipulated in this way in Bob's encoding station is then combined with the other photon at Alice's Bell-state analyzer.

(t2): After Alice receives the photon from Bob, she performs a (partial) Bell measurement on both photons. The Bell-state analyzer consists of a BS followed by two channel PBSs in each of its outputs and proper coincidence analysis between four single-photon detectors. If she obtains a coincidence between detectors D_H and $D_{V'}$ or between $D_{H'}$ and D_V, the result state is $|\Psi^-\rangle_c$. If a coincidence between detectors D_H and D_V or between $D_{H'}$ and $D_{V'}$ is achieved, she obtains the result state $|\Psi^+\rangle_c$. And then she achieves the operator which Bob performed on the travel qubit. If there are other invalid coincidences registered, they will go to step (t1) for the same round again; else, they will go to the next step (see Table I).

(t3): If $n<N$, they go to Step 3; else, the transmission of the N-bit information is completed.

C. Security proof

Now we provide an analysis proposed by Boström *et al.* [25] that guarantees the security of our scheme against arbitrary eavesdropping strategy. Assume that Eve is an eavesdropper whose aim is to find out which operation Bob performs. Since she cannot access Alice's home qubit, the state of the travel qubit is indistinguishable from the complete mixture

$$\rho_A=\mathrm{Tr}_B\{|\Psi^+\rangle_c\langle\Psi^+|\}=\tfrac{1}{2}(|H\rangle_c\langle H|+|V\rangle_c\langle V|), \qquad (17)$$

which corresponds to the situation where Alice sends the travel qubit in either of the states $|H\rangle_c$ or $|V\rangle_c$, with the same probability $\frac{1}{2}$. In order to gain the information about Bob's operation, Eve prepares photons in an ancilla state $|\phi\rangle_c\in H_E$, where H_E is an ancilla space of dimension dim $H_E\leqslant(\dim H_A)^2$. Then, Eve performs a unitary attack operation E on the composed system $\rho_{AE}=\rho_A\otimes|\phi\rangle_c\langle\phi|\in H_E\otimes H_A$.

We choose the case where Bob sends $|H\rangle_c$ by way of example. Eve adds an ancilla state $|\phi\rangle_c$ and performs the unitary operation E on the composed system, resulting in the state

$$|\psi\rangle=E|H\rangle_c\otimes|\phi\rangle_c=\alpha|H,\phi_0\rangle_c+\beta|V,\phi_1\rangle_c, \qquad (18)$$

where $|\phi_0\rangle_c$ and $|\phi_1\rangle_c$ are pure states determined by the operator E, and $|\alpha|^2+|\beta|^2=1$. Hence, the detection probability for Eve's attack is $d=|\beta|^2$. After the attack operation of Eve, the state of the composed system is shown as

$$\rho'_{AE}=|\psi\rangle_c\langle\psi|, \qquad (19)$$

which is usually written in the orthogonal basis $\{|H,\phi_0\rangle_c,|V,\phi_1\rangle_c\}$ as

$$\rho'_{AE}=\begin{pmatrix}|\alpha|^2 & \alpha\beta^* \\ \alpha^*\beta & |\beta|^2\end{pmatrix}. \qquad (20)$$

Bob encodes the information by performing the operation I or σ_z on his photon, with the probability p_0 or p_1, respectively. Then, the state of the composed system is

$$\rho''_{AE} = \begin{pmatrix} |\alpha|^2 & \alpha\beta^*(p_0 - p_1) \\ \alpha^*\beta(p_0 - p_1) & |\beta|^2 \end{pmatrix}. \tag{21}$$

Since a probable detection measurement by Bob takes place before Eve's final measurement, the operation performed by Bob has no influence on the detection probability λ_d for Eve's attack. Now we give the maximal amount I_0 of classical information gain, which can be represented by the von Neumann entropy,

$$I_0 = S(\rho''_{AE}) = -\mathrm{Tr}\{\rho''_{AE}\log_2\rho''_{AE}\} = -\lambda_1\log_2\lambda_1 - \lambda_2\log_2\lambda_2, \tag{22}$$

where $\lambda_{1,2}$ are the two eigenvalues of ρ''_{AE},

$$\lambda_{1,2} = \tfrac{1}{2}\{1 \pm \sqrt{1 - 4|\alpha\beta|^2[1 - (p_0 - p_1)^2]}\} = \tfrac{1}{2} \pm \tfrac{1}{2}\sqrt{1 - (4\lambda_d - 4\lambda_d^2)[1 - (p_0 - p_1)^2]}. \tag{23}$$

The function $I_0(\lambda_d, p_0)$ has a maximum at $\lambda_d = 1/2$, and $p_0 = 1/2$, and for a certain p_0, can be inversed on the interval $[0, 1/2]$, giving a monotonous function $0 \leqslant \lambda_d(I_0) \leqslant 1/2$, $I_0 \in [0, 1]$. By choosing a desired information gain $I_0(\lambda_d) > 0$ per attack, the detection probability $\lambda_d(I_0) > 0$, which means any effective eavesdropping attack can be detected.

V. SUMMARY

Finally, we have a brief conclusion. In this paper, we have studied the possibilities of preparing general entangled states between two different cavities. Then we show one of the applications—secure direct communication allowing asymptotically secure key distribution and quasisecure direct communication. From the application, it is easier to find the following favorable features: First, it is robust to realistic noise and imperfections which only decrease the success probability but have no influence on the fidelity of the EPR state generation. As a result, the physical requirements of this scheme are moderate and well fit the experimental technique. Second, one can store the local qubit in the atomic internal states instead of the photonic states since it is different to store photons for a reasonably long time.

ACKNOWLEDGMENTS

This work was funded by the National Fundamental Research Program (Grant No. 2001CB309300), the National Natural Science Foundation of China, and the Innovation funds from the Chinese Academy of Sciences.

[1] For a review and many references, see H.-I. Yoo, and J. H. Eberly, Phys. Rep. **118**, 239 (1985).
[2] A. S. Parkins, P. Marte, P. Zoller, and H. J. Kimble, Phys. Rev. Lett. **71**, 3095 (1993).
[3] Y. Kaluzny *et al.*, Phys. Rev. Lett. **51**, 1175 (1983); C. W. Gardiner *et al.*, Phys. Rev. A **61**, 045801 (2000); S. J. van Enk *et al.*, *ibid.* **64**, 013407 (2001); P. Munstermann *et al.*, Phys. Rev. Lett. **82**, 3791 (1999); P. Horak *et al.*, *ibid.* **88**, 043601 (2002); A. Kuhn, M. Hennrich, and G. Rempe, *ibid.* **89**, 067901 (2002); M. S. Feld and K. An, Sci. Am. **279** (1), 56 (1998); G. R. Guthohrlein *et al.*, Nature (London) **414**, 49 (2001); A. B. Mundt *et al.*, Phys. Rev. Lett. **89**, 103001 (2001).
[4] C. K. Law and H. J. Kimble, J. Mod. Opt. **44**, 2067 (1997).
[5] K. M. Gheri *et al.*, Phys. Rev. A **58**, R2627 (1998).
[6] C. J. Hood *et al.*, Science **287**, 1447 (2000).
[7] P. W. H. Pinkse *et al.*, Nature (London) **404**, 365 (2000).
[8] A. C. Doherty *et al.*, Phys. Rev. A **63**, 013401 (2000).
[9] J. I. Cirac *et al.*, Phys. Rev. Lett. **78**, 3221 (1997).
[10] S. J. Enk, J. I. Cirac, and P. Zoller, Science **279**, 205 (1998).
[11] C. Cabrillo, J. I. Cirac, P. G. Fernandez, and P. Zoller, Phys. Rev. A **59**, 1025 (1999).
[12] S. Bose, P. L. Knight, M. B. Plenio, and V. Vedral, Phys. Rev. Lett. **83**, 5158 (1999).
[13] M. B. Plenio, S. F. Huelga, A. Beige, and P. L. Knight, Phys. Rev. A **59**, 2468 (1999).
[14] J. Ye, D. W. Vernooy, and H. J. Kimble, Phys. Rev. Lett. **83**, 4987 (1999).
[15] G. R. Guthohrlein *et al.*, Nature (London) **414**, 49 (2001).
[16] J. Eschner, C. H. Raab, F. Schmidt-Kaler, and R. Blatt, Nature (London) **413**, 495 (2001).
[17] J. M. Raimand, M. Brune, and S. Haroche, Rev. Mod. Phys. **73**, 565 (2001).
[18] E. Hagley *et al.*, Phys. Rev. Lett. **79**, 1 (1997).
[19] A. Rauschenbeutel *et al.*, Science **288**, 2024 (2000).
[20] S.-B. Zheng and G.-C. Guo, Phys. Rev. Lett. **85**, 2392 (2000).
[21] A. S. Sorensen and K. Molmer, e-print quant-ph/0304008.
[22] A. S. Sorensen and K. Molmer, Phys. Rev. A **66**, 022314 (2002).
[23] L.-M. Duan and H. J. Kimble, e-print quant-ph/0301164.
[24] M. B. Plenio, D. E. Browne, and S. F. Huelga, e-print quant-ph/0302185.
[25] K. Boström and T. Felbinger, Phys. Rev. Lett. **89**, 187902 (2002).
[26] In order to detect the eavesdropping proposed by A. Wójcik [Phys. Rev. Lett. **90**, 157901 (2003)], Bob should delay the announcement of the information about a chosen mode. Note that Eve's action depends on the actual Bob's choice of the communication mode. In the next step, Alice has also to check if there is any photon in the transmission mode. In this way, the detection of eavesdropping based on the analysis restrict the detection mode can be achieved.