Bidirectional quantum key distribution protocol with practical faint laser pulses

Fu-Guo Deng[1,2] and Gui Lu Long[1,2,3,4]

[1]*Department of Physics, Tsinghua University, Beijing 100084, China*
[2]*Key Laboratory for Quantum Information and Measurements, Beijing 100084, China*
[3]*Center for Atomic and Molecular NanoSciences, Tsinghua University, Beijing 100084, China*
[4]*Center for Quantum Information, Tsinghua University, Beijing, 100084, China*

(Received 4 March 2004; published 20 July 2004)

We present a two-way protocol for the quantum key distribution with practical faint laser pulses. It is secure when the faint laser pulses contain no more than two photons. The key distribution task is completed in two transmissions. Bob first sends the laser pulses to Alice, and Alice encodes the key message through certain unitary operations and returns the laser pulses to Bob. Security is achieved by placing eavesdropping check procedures in both transmissions. This protocol is secure and is close to practical conditions. In addition, it does not require the exchange of measuring basis information between Alice and Bob, hence saving a lot of storage space.

DOI: 10.1103/PhysRevA.70.012311 PACS number(s): 03.67.Dd, 03.67.Hk

I. INTRODUCTION

Preventing information from leaking to an eavesdropper has become one of the most important issues nowadays. The known way to complete the task securely through a communication channel is the one-time pad cryptosystem in which the secret message represented by a string of classical bits is combined with a key composed of a sequence of random binary numbers with equal length. The randomness of the key ensures that the cryptogram obtained by encoding the secret message with the key is also completely random and as such totally unintelligible to other unauthorized users. The security of the key distribution is the core part in secret communications. There is no way for creating a key unconditionally secure with classical signals as an eavesdropper, Eve, can monitor the line freely without leaving a trace. When quantum mechanics enters the field of information, the case is changed and the quantum key distribution (QKD), a mature application of the principles in quantum mechanics such as the uncertainty principle, quantum correlations, and nonlocality, supplies a secure way for generating a key privately and has progressed quickly [1–9] since Bennett and Brassard designed an original QKD protocol (BB84 protocol) [10] based on a noncloning theorem [11] with polarized single photons in 1984. Though the QKD is usually based on single photons, recently QKD's based on continuous variables are being actively explored [7–9]; they offer a potential higher key distribution rate. They can be implemented with practical faint laser pulses and homodyne detectors, which is practically attractive.

For a secure communication with BB84 protocol, a perfect single-photon source is required. Although single photons can be produced in principle [13], there is still some distance away from practical application. The demonstration of QKD protocols has been done with faint laser pulses [14,15]. It is very likely that the first commercial QKD machines will use attenuated laser pulses instead of perfect single-photon sources, though in most laser pulses there is only a single photon, but there is still some probability that the pulse may contain more than two photons. Hence there is a serious threat as Eve can use photon-number splitting (PNS) attacks [16] to steal a fraction of the information about the key.

In this paper, we will present a practical bidirectional QKD scheme. This QKD protocol is based on a recent secure quantum direct communication protocol using perfect single-photon sources [12]. It has several distinct features. First, as in the direct secure quantum protocol [12], it does not require the exchange of the measuring-basis information, and it saves a lot of on-site classical information storage and reduces the classical communication cost. Second, it is secure even for laser pulses that contain two single photons. With a perfect single-photon source, this QKD protocol is secure. As the protocol uses bidirectional transmissions, it is secure even when the single photons are replaced by faint laser pulses that do not contain more than two single photons. This greatly relieves the demand on the single-photon source. This will allow us to use less attenuation in the laser pulse and helps to increase the communication distance. We will give the details of the protocol in Sec. II and the security analysis is given in Sec. III. In Sec. IV, we give a brief summary.

II. BIDIRECTIONAL QKD PROTOCOL

A. Property of faint laser pulses

Laser lights are coherent states, and they can be produced without difficulty. In the QKD, single photons are approximated by faint laser pulses that are obtained after performing an attenuation to an extent that the mean photon number in each pulse is less than 0.1. The coherent state gives a Poisson distribution in the Fock states, the number states. The probability that there are n single photons in a pulse is [1]

$$P(n) = \frac{\alpha^n}{n!} e^{-\alpha}, \tag{1}$$

where n is the photon number and $\alpha = \langle |n| \rangle$ is the average number of photons in a pulse. Then the probabilities that a nonempty weak coherent pulse contains more than one and two photons can be calculated, respectively, as follows [1]:

$$P(n>1|n>0) = \frac{1-P(0)-P(1)}{1-P(0)} = \frac{1-(1+\alpha)e^{-\alpha}}{1-e^{-\alpha}} \cong \frac{\alpha}{2}, \tag{2}$$

$$\begin{aligned} P(n>2|n>0) &= \frac{1-P(0)-P(1)-P(2)}{1-P(0)} \\ &= \frac{1-\left(1+\alpha+\dfrac{\alpha^2}{2}\right)e^{-\alpha}}{1-e^{-\alpha}} \cong \frac{\alpha^2}{3}. \end{aligned} \tag{3}$$

If $\alpha=0.05$, the probabilities $P(n>1|n>0)\approx 2.5\times 10^{-2}$ and $P(n>2|n>0)\approx 8.3\times 10^{-4}$, respectively. That is, when the Fock states are attenuated to one photon per 20 pulses, the probability that there are more than two photons in a pulse is about 10^{-3}.

In the implementation of the BB84 protocol with faint laser pulses, it is well known that there is danger if there are two photons in a pulse. Eve can eavesdrop on the communication with PNS attacks [16]. That is, Eve splits one photon in a multiphoton pulse and gets a deterministic outcome. Then Eve can steal some information about the key, and Alice and Bob cannot detect the action of Eve. The attack can be avoided by using perfect single-photon sources. However, at present, perfect single photons are some distance away from practical application; to avoid this type of attack, it is necessary to lower the average number in a pulse. By doing so, the laser pulses are very weak.

III. QKD PROTOCOL

The bidirectional QKD protocol is a modification to the quantum secure direct communication protocol [12] where the ideas from dense coding [4] and the BB84 QKD protocol [10] are combined. In the QKD, the security requirement is less than that of the direct secure communication where both the capability of detecting Eve and the capability of not leaking secret information before detecting Eve are required. In the QKD, only the capability to detect Eve is required because, once Eve is found, Alice and Bob can simply discard the raw key. The detailed procedures for the bidirectional QKD protocol is as follows.

(1) The receiver, Bob, chooses randomly two conjugate bases: the rectilinear basis (i.e., $\{|H\rangle=|0\rangle, |V\rangle=|1\rangle\}$) and diagonal basis [i.e., $\{|u\rangle=(1/\sqrt{2})(|0\rangle+|1\rangle), |d\rangle=(1/\sqrt{2})(|0\rangle-|1\rangle)\}$] to produce each faint laser pulse randomly in one of the states and sends the laser pulses to Alice. Here $|H\rangle$ and $|V\rangle$ denote the horizontal and vertical linear polarizations of photons, respectively.

(2) Upon receiving the laser pulses, Alice decides to pick up the coding mode or checking mode for each pulse. If she selects the checking mode, she performs the measurement on the quantum signal choosing randomly one of the two bases and then tells Bob which photon she has sampled for measurement and the information about the measuring basis and outcome. With this knowledge, Bob can check if Alice's measurement is consistent with his in those cases where Alice chooses the same measuring basis as his. This is equivalent to the eavesdropping check of the BB84 QKD protocol.

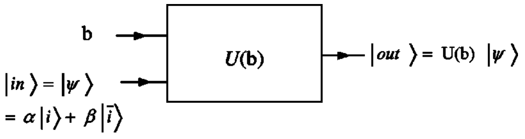
b
$|in\rangle=|\psi\rangle$
$=\alpha|i\rangle+\beta|\bar{i}\rangle$
U(b)
$|out\rangle=$ U(b) $|\psi\rangle$

FIG. 1. Coding with the quantum operation.

If Alice chooses the coding mode, she encodes on the quantum signal with one of the two unitary operations randomly, where $U(b)$ is defined as

$$U(b) = \frac{I+i\sigma_y}{2} + (-1)^b \frac{I-i\sigma_y}{2}, \tag{4}$$

and $b\in\{0,1\}$ is the binary number that Alice wants to transmit to Bob. The output state after $U(b)$ for a input state $|\psi\rangle = \alpha|i\rangle+\beta|\bar{i}\rangle$ is

$$U(b)|\psi\rangle = \alpha(-1)^{b(b\oplus i)}|i\oplus b\rangle + \beta(-1)^{b(b\oplus\bar{i})}|\bar{i}\oplus b\rangle, \tag{5}$$

and $i\in\{0,1\}$ and $|\alpha|^2+|\beta|^2=1$, shown in Fig. 1. Explicitly $U(0)=I=|0\rangle\langle 0|+|1\rangle\langle 1|$ and $U(1)=|0\rangle\langle 1|-|1\rangle\langle 0|$. The effect of the operator $U(1)$ is only to negate (e.g., $0\rightarrow 1, 1\rightarrow 0$) the quantum states in the same measuring basis—i.e.,

$$U(1)|H\rangle = -|V\rangle, \tag{6}$$

$$U(1)|V\rangle = |H\rangle, \tag{7}$$

$$U(1)|u\rangle = |d\rangle, \tag{8}$$

$$U(1)|d\rangle = -|u\rangle. \tag{9}$$

After encoding the quantum signal, Alice returns it to Bob.

(3) After receiving the pulses from Alice, Bob performs the measurement using the measuring basis he previously used to read out the information about Alice's operations. The schematic demonstration is shown in Fig. 2.

After transmitting a sufficiently large set of qubits, Bob does the analysis on the results which will be divided into three sequences. The first one is those Alice has chosen in the checking mode and with the same measuring basis as Bob. This checking can find out whether the eavesdropper, Eve, takes the quantum operation on the quantum signal if the laser pulses contain only a single photon. However, if there are more than two photons in a pulse, Eve can use the PNS attacks [16] in the transmission from Bob to Alice, and Eve's PNS attack can evade this first check. The second part is chosen by Bob randomly from the results for which Alice has chosen the encoding mode and has done the encoding operation. Bob publishes the results of this part, and by comparison Alice and Bob can check if Eve is present in the transmission from Alice to Bob. The third part is the biggest part of the results and Bob can use them as the key for later encryption; of course, some post-processing has to be done if there are noises.

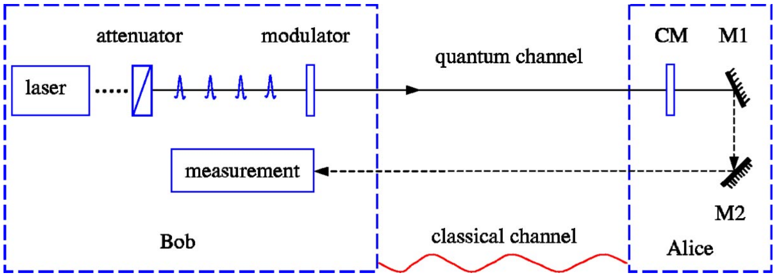

FIG. 2. Schematic realization of the QKD protocol. CM determines to use the checking mode or coding mode; M1 and M2 are two mirrors for returning the quantum signals.

The security of this QKD protocol depends on the two processes of eavesdropping checking. If the quantum signal is perfect single photons, then the QKD communication is unconditionally secure which is the same as that for the BB84 QKD protocol [17], because it is equivalent to Alice and Bob doing the two BB84 QKD processes. Second, because there are two eavesdropping checks, laser pulses containing no more than two photons can be used securely. Even though Eve can use the PNS attack during the transmission from Bob to Alice, the second check will discover Eve. There are several advantages to this protocol. First the intrinsic efficiency of this protocol is high as every photon is used for the valid key distribution except those chosen for the eavesdropping check. Moreover, it is not necessary for Alice and Bob to exchange information about the measuring bases for the photons.

IV. SECURITY ANALYSIS OF THE BIDIRECTIONAL QKD PROTOCOL

A. Proof of the security with a perfect single-photon source

There are a lot of attack methods done by Eve. For stealing all the information that Alice encodes on the quantum signal, Eve introduces the error rate in the results no more than 25% which is the limitation done by intercept-resend attack strategy. That is, Eve intercepts all the particles prepared by Bob and sends a sequence of fake particles to Alice. After the coding done by Alice with quantum operation $U(b)$, Eve measures the particles one by one, and obtains the information completely. She will introduce 25% error rate in the results of the first checking eavesdropping.

Without loss of generality, we now work with the assumption that Eve can only be able to make individual attacks. In this time, the quantum signal is the perfect single-photon source. The optimal individual attack done by Eve can be realized by a unitary operation [6,18–22] on the photon traveling with a probe whose initial state is $|0\rangle$—i.e.,

$$U_{TE}|\xi\rangle|0\rangle = |\xi\rangle|0\rangle, \tag{10}$$

$$U_{TE}|\overline{\xi}\rangle|0\rangle = \cos\,\phi|\overline{\xi}\rangle|0\rangle + \sin\,\phi|\xi\rangle|1\rangle, \tag{11}$$

where $|\xi\rangle$ and $|\overline{\xi}\rangle$ are two eigenvectors of the two-level operator [18,19], and $\phi \in [0,\pi/4]$ characterizes the strength of Eve's attack [6].

For Alice and Bob, Eve's eavesdropping will introduce the error rate

$$\varepsilon = P_{\overline{\xi}}\sin^2\phi, \tag{12}$$

where $P_{\overline{\xi}}$ is the probability that the quantum signal is in state $|\overline{\xi}\rangle$. Let us suppose that $|\xi\rangle = |0\rangle$ and $|\overline{\xi}\rangle = |1\rangle$ are the eigenvectors of σ_z (the condition that they are eigenstates of σ_x is the same as it for checking eavesdropping):

$$U_{TE}|0\rangle|0\rangle = |0\rangle|0\rangle \equiv |00\rangle, \tag{13}$$

$$U_{TE}|1\rangle|0\rangle = \cos\,\phi|1\rangle|0\rangle + \sin\,\phi|0\rangle|1\rangle \equiv \cos\,\phi|10\rangle + \sin\,\phi|01\rangle, \tag{14}$$

$$\varepsilon = \frac{1}{2}\sin^2\phi. \tag{15}$$

Bob prepares the photon in each state with equal probability; the density matrix of the quantum signal for Eve is

$$\rho_P = \frac{1}{4}|H\rangle\langle H| + \frac{1}{4}|V\rangle\langle V| + \frac{1}{4}|u\rangle\langle u| + \frac{1}{4}|d\rangle\langle d| = \frac{1}{2}|0\rangle\langle 0| + \frac{1}{2}|1\rangle \times\langle 1|. \tag{16}$$

Before the coding done by Alice, the quantum states carry no useful information for Eve and Bob. On the other hand, without eavesdropping the quantum signal, Eve cannot distinguish the quantum operations done by Alice on the states, which is the same as the classical one-time-pad cryptosystem. That is to say, she has to eavesdrop the quantum signals running forth and back. The information I_E about the quantum operations (or the code done by Alice) that Eve can obtain is less than the minimum number in the information from the quantum signal forth and back—say, I_{Ef} and I_{Eb}:

$$I_E \leqslant \min(I_{Ef}, I_{Eb}). \tag{17}$$

But the error rate ε introduced by her disturbance is more than the maximal one of ε_{Ef} and ε_{Eb} which are the error rates in the two checking eavesdropping processes, respectively:

$$\varepsilon \geqslant \max(\varepsilon_{Ef}, \varepsilon_{Eb}). \tag{18}$$

I_{Ef}, I_{Eb} and ε_{Ef}, ε_{Eb} can be calculated similarly.

After Eve's eavesdropping, the state of the system composed of the photon and Eve's probe can be described by

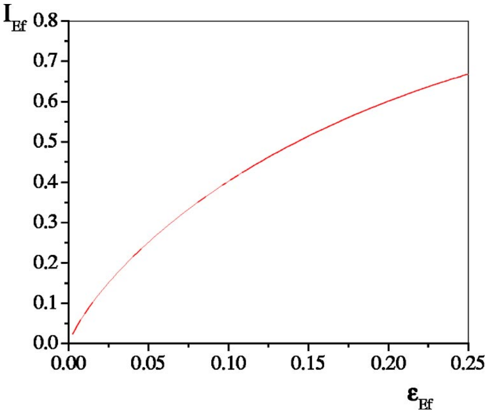

FIG. 3. The relation between information obtained by Eve, I_{Ef}, and the error rate introduced by her, ε_{Ef}.

$$\rho_s' = \frac{1}{2}[|00\rangle\langle 00| + \cos^2\phi|10\rangle\langle 10| + \sin^2\phi|01\rangle\langle 01| + \cos\phi\sin\phi|10\rangle\langle 01| + \cos\phi\sin\phi|01\rangle\langle 10|]. \tag{19}$$

Tracing out the photon from the system ρ_s', we can get the density matrix of Eve's probe ρ_{Ef}:

$$\rho_{Ef} = \frac{1}{2}\begin{pmatrix} 1+\cos^2\phi & 0 \\ 0 & \sin^2\phi \end{pmatrix}. \tag{20}$$

The information I_{Ef} about the quantum states of the quantum signal prepared by Bob, which Eve can get, is equal to the Von Neumann entropy [20]

$$I_{Ef} = S(\rho_E) = -\,\mathrm{Tr}(\rho_{Ef}\log_2\rho_{Ef}), \tag{21}$$

i.e.,

$$I_{Ef} = S(\rho_{Ef}) = -\sum_{i=0}^{1}\lambda_i\log_2\lambda_i, \tag{22}$$

where λ_i $(i=0,1)$ are the eigenvalues of ρ_{Ef}, which are $\lambda_0 = \frac{1}{2}(1+\cos^2\phi)$ and $\lambda_1 = \frac{1}{2}\sin^2\phi$. That is to say,

$$I_{Ef} = 1 - \frac{1}{2}[(1+\cos^2\phi)\log_2(1+\cos^2\phi) + \sin^2\phi\,\log_2\sin^2\phi] = -\,\varepsilon_{Ef}\log_2\varepsilon_{Ef} - \left(1-\frac{\varepsilon_{Ef}}{2}\right)\log_2\left(1-\frac{\varepsilon_{Ef}}{2}\right). \tag{23}$$

The relation between I_{Ef} and ε_{Ef} is shown in Fig. 3. Undergoing the first eavesdropping done by Eve, the state of the photon traveling reads

$$\rho_P' = \frac{1}{2}[(1+\sin^2\phi)|0\rangle\langle 0| + \cos^2\phi|1\rangle\langle 1|], \tag{24}$$

which is obtained by means of tracing out the probe of Eve's from the system.

After coding $U(0)$ and $U(1)$ with equal probabilities, the state becomes

$$\rho_P'' = \frac{1}{2}[|0\rangle\langle 0| + |1\rangle\langle 1|]. \tag{25}$$

Suppose that Eve uses the same attack strategy (the optimal individual attack) in the second eavesdropping as she does for the quantum signal traveling from Bob to Alice. A similar result can be obtained easily—i.e.,

$$I_{Eb} = 1 - \frac{1}{2}[(1+\cos^2\varphi)\log_2(1+\cos^2\varphi) + \sin^2\varphi\,\log_2\sin^2\varphi] = -\,\varepsilon_{Eb}\log_2\varepsilon_{Eb} - \left(1-\frac{\varepsilon_{Eb}}{2}\right)\log_2\left(1-\frac{\varepsilon_{Eb}}{2}\right), \tag{26}$$

where $\varphi \in [0,\pi/4]$, similar to ϕ, used to characterize the strength of the second attack done by Eve [6]. I_{Eb} and ε_{Eb} have the same relation as I_{Ef} and ε_{Ef}.

With a quantum channel whose noise does not contribute to the error rate largely, the disturbance of Eve's eavesdropping is detected easily. Moreover, Eve can get the information less than the mutual information between Alice and Bob, $I(A:B)$, which is 1 bit for each photon.

In a word, this protocol is secure if there is no more than one photon in a pulse same as that in Ref. [10]. The analysis of the error rates will discover the action of Eve during the photons traveling from Bob to Alice or returning back. In fact, Alice and Bob use a maximally mixed-state traveling through the insecure quantum channel, which makes Eve leave a trick in the results if she monitors the channel.

B. Security analysis with faint laser pulses with no more than two photons

For a faint laser pulse source, there is just no more than one photon in a pulse in the most time and at this time it can be considered as a perfect single-photon source. On the other hand, there is a small probability that the pulse includes more than one photon. As discussed above, when $\alpha=0.05$, the probabilities $P(n>1|n>0) \approx 2.5\times 10^{-2}$ and $P(n>2|n>0) \approx 8.3\times 10^{-4}$, respectively. As the probability of loss for each photon in the quantum channel cannot be thought of as different, there are no more than 3% probability for Eve to eavesdrop on the quantum communication with PNS attacks. Moreover, the attacks on the pulse that includes only two photons will leave a trick, which is different from the BB84 QKD protocol [10]. When there are more than two photons in a pulse, the probability that Eve attacks the communication successfully will increase. However, the probability of this taking place the instance is as small as the probability that a pulse includes more than two photons is less than 10^{-3}. On the one hand, Eve cannot obtain the information about the quantum operation done by Alice perfectly as she does not know the base for each pulse because they do not publish them, and the number of photons in the same quantum states which is unknown to Eve is limited, and she cannot copy them fully [11]. On the other hand, Alice and Bob can do privacy amplification to eliminate the information leaked to

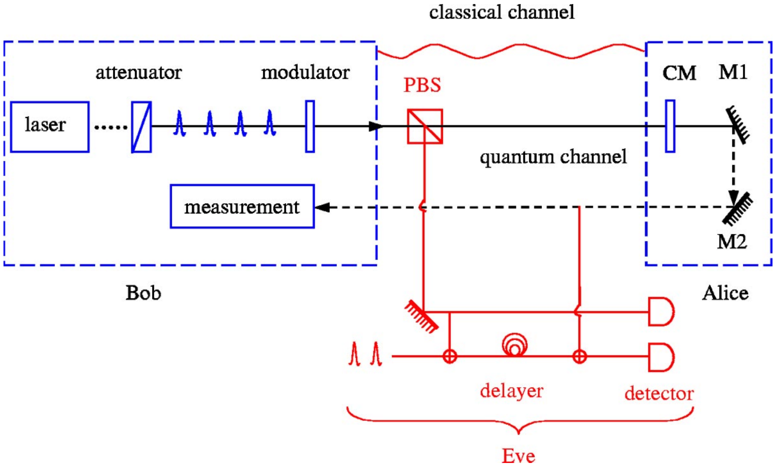

FIG. 4. Schematic demonstration of this QKD protocol with eavesdropping using the CNOT operation when there are no more than two photons in a pulse. PBS is a photon beam splitter.

Eve. So this protocol for the QKD with a faint laser pulse is secure.

Now, let us first discuss the case that there are two photons in a pulse, which happens with not a negligible probability if α is not too small. In this case, PNS attacks [16] can be used by the means that Eve captures a photon from the pulse composed of multiphotons when they travel from Bob to Alice, shown in Fig. 4. His action, of course, will increase the lossy rate of the quantum signal, but he can eavesdrop on a fraction of the quantum signal and use a better quantum channel to transmit the other quantum signal in order to make the loss of photons change nothing, which does not violate the nature. After Alice's coding, he intercepts the quantum signal to eavesdrop on the information about the coding done by Alice. In this way, the goal of the attacks is to distinguish the quantum states of the two photons having different stories in the originally same pulse and not leave a trick in the results.

Eve cannot perform measurements of the quantum signal returning from Alice to Bob simply as she does not know the measuring bases and any measurement done by Eve will introduce errors in the results similar to that in the BB84 QKD protocol [10] with a perfect single photon source. Moreover, any eavesdropping on the traveling quantum signal can be considered as an unitary operation, which will leave a trick on the results and be detected when Alice and Bob do the second eavesdropping check, the same as that with only one photon in a pulse discussed above.

As an example of the attack, let us assume that Eve uses as control not (CNOT) operation (presented in Fig. 2) to distinguish the two photons having different stories in a pulse. As Eve cannot measure the quantum signal back from Alice, this eavesdropping does not succeed. We give the reason as follows.

Suppose the state that Eve inputs in CNOT gate acting as target bit is $|t\rangle = a_1|0\rangle + b_1|1\rangle$, and the photon (the first control bit) she captures with the photon beam splitter (PBS) is in the state $|c_2\rangle = a_2|0\rangle + b_2|1\rangle$, where $|a_1|^2 + |b_1|^2 = 1$ and $|a_2|^2 + |b_2|^2 = 1$. The state of the joint system composed of the control bit and target bit can be written as a product state as follows:

$$|\psi\rangle_{c_2t} = (a_2|0\rangle + b_2|1\rangle) \otimes (a_1|0\rangle + b_1|1\rangle) = a_2a_1|00\rangle + a_2b_1|01\rangle + b_2a_1|10\rangle + b_2b_1|11\rangle. \tag{27}$$

After the CNOT gate, the state reads

$$|\psi'\rangle_{c_2t} = a_2a_1|00\rangle + a_2b_1|01\rangle + b_2a_1|11\rangle + b_2b_1|10\rangle = a_2|0\rangle \times (a_1|0\rangle + b_1|1\rangle) + b_2|1\rangle(a_1|1\rangle + b_1|0\rangle). \tag{28}$$

When the traveling quantum signal is encoded in the state $|c_3\rangle = a_3|0\rangle + b_3|1\rangle$, Eve intercepts it as the second control bit to do the CNOT operation on the target bit. Then the state of the system made up of three particles is

$$\begin{aligned}|\psi'\rangle_{c_3c_2t} &= (a_3|0\rangle + b_3|1\rangle) \otimes [a_2|0\rangle(a_1|0\rangle + b_1|1\rangle) + b_2|1\rangle(a_1|1\rangle \\ &\quad + b_1|0\rangle)] = a_3|0\rangle a_2|0\rangle(a_1|0\rangle + b_1|1\rangle) + a_3|0\rangle b_2|1\rangle \\ &\quad \times (a_1|1\rangle + b_1|0\rangle) + b_3|1\rangle a_2|0\rangle(a_1|0\rangle + b_1|1\rangle) \\ &\quad + b_3|1\rangle b_2|1\rangle(a_1|1\rangle + b_1|0\rangle).\end{aligned} \tag{29}$$

Completing the CNOT operation, the state becomes

$$\begin{aligned}|\psi''\rangle_{c_3c_2t} &= a_3|0\rangle a_2|0\rangle(a_1|0\rangle + b_1|1\rangle) + a_3|0\rangle b_2|1\rangle(a_1|1\rangle \\ &\quad + b_1|0\rangle) + b_3|1\rangle a_2|0\rangle(a_1|1\rangle + b_1|0\rangle) + b_3|1\rangle b_2|1\rangle \\ &\quad \times (a_1|0\rangle + b_1|1\rangle) = (a_3a_2|0\rangle|0\rangle + b_3b_2|1\rangle|1\rangle)(a_1|0\rangle \\ &\quad + b_1|1\rangle) + (a_3b_2|0\rangle|1\rangle + b_3a_2|1\rangle|0\rangle)(a_1|1\rangle + b_1|0\rangle).\end{aligned} \tag{30}$$

The results of the CNOT operation is shown in Table I, which tells us that the eavesdropping done by Eve with the CNOT operation cannot distinguish the difference between the original and coding quantum signals because of the principle of superposition. Moreover, her action disturbs the quantum signal and will be detected in the second check.

If there are more than two photons in a pulse, Eve, of course, can eavesdrop without introducing errors in the results of the communication, shown in Fig. 5. But it is difficult to distinguish the two states before and after the coding perfectly. Eve can measure them with a same basis choosing randomly and have not less than 75% probability to obtain the information if she can capture one photon before and after the coding, respectively. With a low-loss quantum channel, the fraction of the quantum signal that can be eavesdropped is smaller; otherwise, the action will make the rate of lossy photons increase largely. As the probability that there are more than two photons in a pulse is very small and

TABLE I. The results of the CNOT operations. ψ (original) and ψ (coding) are the states originally prepared by Bob and those after the coding done by Alice, respectively.

Coding operation	ψ (coding)	ψ (original)	$\psi_{c_3c_2t}$
I	$\|1\rangle$	$\|1\rangle$	$\|1\rangle\|1\rangle(a_1\|0\rangle+b_1\|1\rangle)$
U	$\|0\rangle$	$\|1\rangle$	$\|0\rangle\|1\rangle(a_1\|1\rangle+b_1\|0\rangle)$
I	$\|0\rangle$	$\|0\rangle$	$\|0\rangle\|0\rangle(a_1\|0\rangle+b_1\|1\rangle)$
U	$-\|1\rangle$	$\|0\rangle$	$-\|1\rangle\|0\rangle(a_1\|1\rangle+b_1\|0\rangle)$
I	$1/\sqrt{2}(\|0\rangle+\|1\rangle)$	$1/\sqrt{2}(\|0\rangle+\|1\rangle)$	$\frac{1}{2}(\|0\rangle\|0\rangle+\|1\rangle\|1\rangle)(a_1\|0\rangle+b_1\|1\rangle)+\frac{1}{2}(\|0\rangle\|1\rangle$ $+\|1\rangle\|0\rangle)(a_1\|1\rangle+b_1\|0\rangle)$
U	$1/\sqrt{2}(\|0\rangle-\|1\rangle)$	$1/\sqrt{2}(\|0\rangle+\|1\rangle)$	$\frac{1}{2}(\|0\rangle\|0\rangle-\|1\rangle\|1\rangle)(a_1\|0\rangle+b_1\|1\rangle)+\frac{1}{2}(\|0\rangle\|1\rangle$ $-\|1\rangle\|0\rangle)(a_1\|1\rangle+b_1\|0\rangle)$
I	$1/\sqrt{2}(\|0\rangle-\|1\rangle)$	$1/\sqrt{2}(\|0\rangle-\|1\rangle)$	$\frac{1}{2}(\|0\rangle\|0\rangle+\|1\rangle\|1\rangle)(a_1\|0\rangle+b_1\|1\rangle)-\frac{1}{2}(\|0\rangle\|1\rangle$ $+\|1\rangle\|0\rangle)(a_1\|1\rangle+b_1\|0\rangle)$
U	$-1/\sqrt{2}(\|0\rangle+\|1\rangle)$	$1/\sqrt{2}(\|0\rangle-\|1\rangle)$	$\frac{1}{2}(-\|0\rangle\|0\rangle+\|1\rangle\|1\rangle)(a_1\|0\rangle+b_1\|1\rangle)+\frac{1}{2}(\|0\rangle\|1\rangle$ $-\|1\rangle\|0\rangle)(a_1\|1\rangle+b_1\|0\rangle)$

Eve cannot obtain the information perfectly, even she can steal two photons from a pulse. Moreover, Alice and Bob can eliminate the information leaked to Eve with the process of privacy amplification. In this way, the protocol is secure for the QKD with faint laser pulses.

V. DISCUSSION AND CONCLUSION

The BB84 QKD protocol is not unconditionally secure with faint laser pulses, especially in a high-loss quantum channel, as Eve can eavesdrop on the communication using PNS attacks [16]. In essence, the demerit comes mainly from the process that Alice and Bob must publish their measuring bases for the quantum signal. If they do not need to announce it, the security of QKD protocol will increase largely.

We present a QKD protocol without announcing the information about the measuring bases. It can be done by the means that the two parties of communication make the quantum signal travel twice distance between them and exploit the quantum operation to code the signal. That is, the receiver, Bob, prepares the quantum signal, randomly choosing the two bases, and sends it to the sender, Alice, and she selects the checking mode or coding mode to operate the quantum signal. If Alice chooses the coding mode, she performs the two unitary operations on the signal with equal probability and then sends it back to Bob. Otherwise, she measures it choosing randomly the two bases and tells Bob all the information about the measurement. After twice checking eavesdropping, they can determine whether there is an eavesdropper in the line for almost all of the instances.

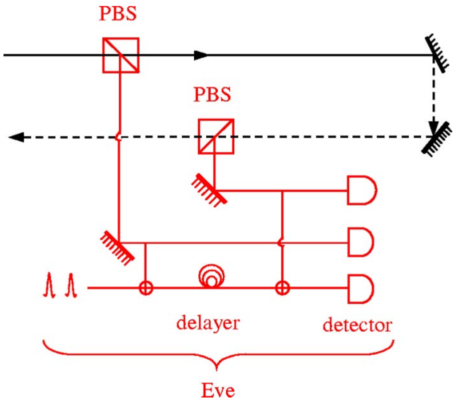

FIG. 5. Eavesdropping using PNS attacks when there are more than two photons in a pulse. PBS is a photon beam splitter.

With a perfect single-photon source, its security is same as the BB84 QKD protocol [10] which is proved unconditionally secure [17]. The advantage of this protocol is that each photon can carry one qubit of information and none of photons are discarded. Moreover, it is not necessary for Alice and Bob to exchange the information about the measuring bases for the photons.

If the quantum signal is the faint laser pulses with small mean photon number α, this protocol is secure with the process of privacy amplification. Moreover, Eve cannot obtain a perfect result even though there are more than two photons in the pulse as the measuring bases are not published.

This protocol is not only suitable for the case with two bases, but also for cases with nonorthogonal states, such as three bases or two nonorthogonal states similar to the six-state protocol [23] and Bennett 1992 protocol [24], respectively.

ACKNOWLEDGMENTS

This work was supported by National Fundamental Research Program Grant No. 001CB309308, China National Natural Science Foundation Grant Nos. 60073009 and 10325521, the Hang-Tian Science Fund, and the SRFDP program of the Education Ministry of China.

[1] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Rev. Mod. Phys. **74**, 145 (2002), and references therein.

[2] A. K. Ekert, Phys. Rev. Lett. **67**, 661 (1991).

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

[4] C. H. Bennett and S. J. Wiesner, Phys. Rev. Lett. **69**, 2881 (1992).

[5] G. L. Long and X. S. Liu, Phys. Rev. A **65**, 032302 (2002); F. G. Deng, X. S. Liu, Y. J. Ma, L. Xiao, and G. L. Long, Chin. Phys. Lett. **19**, 893 (2002); F. G. Deng and G. L. Long, Phys. Rev. A **68**, 042315 (2003).

[6] V. Scarani and N. Gisin, Phys. Rev. Lett. **87**, 117901 (2001).

[7] Ch. Silberhorn, T. C. Ralph, N. Lütkenhaus, and G. Leuchs, Phys. Rev. Lett. **89**, 167901 (2002).

[8] T. Hirano, H. Yamanaka, M. Ashikaga, T. Konishi, and R. Namiki, Phys. Rev. A **68**, 042331 (2003).

[9] F. Grosshans, G. Van Assche, J. Wenger, R. Brouri, N. J. Cerf, and P. Grangier, Nature (London) **421**, 238 (2003).

[10] C. H. Bennett and G. Brassard, in *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India* (IEEE, New York, 1984), pp. 175–179.

[11] W. K. Wootters and W. H. Zurek, Nature (London) **299**, 802 (1982).

[12] F. G. Deng and G. L. Long, Phys. Rev. A **69**, 052319 (2004).

[13] For a review, see C. Brunel, B. Lounis, P. Tamarat, and M. Orrit, Phys. Rev. Lett. **83**, 2722 (1999); P. Michler, A. Kiraz, C. Becher, W. V. Schoenfeld, P. M. Petroff, L. Zhang, E. Hu, and A. Imamoğlu, Science **290**, 2282 (2000); Z. Yuan, B. E. Kardynal, R. M. Stevenson, A. J. Shields, C. J. Lobo, K. Cooper, N. S. Beattie, D. A. Ritchie, and M. Pepper, *ibid.* **295**, 102 (2002); A. Kuhn, M. Hennrich, and G. Rempe, Phys. Rev. Lett. **89**, 067901 (2002); A. L. Migdall, D. Branning, and S. Castelletto, Phys. Rev. A **66**, 053805 (2002); W. Nakwaski, R. P. Sarzała, M. Wasiak, T. Czyszanowski, and P. Maćkowiak, Opto-Electron. Rev. **11(2)**, 127 (2003).

[14] For a review, see C. H. Bennett, F. Besette, G. Brassard, L. Salvail, and J. Smolin, J. Cryptogr. **5**, 3 (1992), or [1] and the references therein.

[15] A. Muller, T. Herzog, B. Huttner, W. Tittel, H. Zbinden, and N. Gisin, Appl. Phys. Lett. **70**, 793 (1996).

[16] B. Huttner, N. Imoto, N. Gisin, and T. Mor, Phys. Rev. A **51**, 1863 (1995); H. P. Yuen, Quantum Semiclassic. Opt. **8**, 939 (1996); N. Lütkenhaus, Phys. Rev. A **61**, 052304 (2000); G. Brassard, N. Lütkenhaus, T. Mor, and B. C. Sanders, Phys. Rev. Lett. **85**, 1330 (2000); N. Lütkenhaus and M. Jahma, New J. Phys. **4**, 44 (2002); W. Y. Hwang, Phys. Rev. Lett. **91**, 057901 (2003).

[17] D. Mayers, e-print quant-ph/9802025; P. W. Shor and J. Preskill, Phys. Rev. Lett. **85**, 441 (2000); D. Mayers, Eur. Phys. J. D **18**, 161 (2002); E. Biham, M. Boyer, P. O. Boykin, T. Mor, and V. Roychowdhury, e-print quant-ph/9912053; N. Lütkenhaus, Phys. Rev. A **61**, 052304 (2000); M. Koashi and J. Preskill, e-print quant-ph/0208155; D. Gottesman, H. K. Lo, N. Lütkenhaus, and J. Preskill, e-print quant-ph/0212066.

[18] C. A. Fuchs, N. Gisin, R. B. Griffiths, C. S. Niu, and A. Peres, Phys. Rev. A **56**, 1163 (1997).

[19] A. Sen(De), U. Sen, and M. Żukowski, Phys. Rev. A **68**, 032309 (2003).

[20] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, Cambridge, UK, 2000).

[21] F. G. Deng, G. L. Long, and X. S. Liu, Phys. Rev. A **68**, 042317 (2003).

[22] H. Inamori, L. Rallan, and V. Vedral, J. Phys. A **34**, 6913 (2001).

[23] B. Huttner, N. Imoto, N. Gisin, and T. Mor, Phys. Rev. A **51**, 1863 (1995).

[24] C. H. Bennett, Phys. Rev. Lett. **68**, 3121 (1992).