Decoy states for quantum key distribution based on decoherence-free subspaces

Zhen-Qiang Yin, Yi-Bo Zhao, Zheng-Wei Zhou,* Zheng-Fu Han,† and Guang-Can Guo
Key Laboratory of Quantum Information, University of Science and Technology of China, Hefei 230026, China
(Received 11 March 2008; published 17 June 2008)

A quantum key distribution with decoherence-free subspaces has been proposed to overcome collective noise to the polarization modes of photons flying in quantum channels. Prototypes of this scheme have also been achieved with a parametric down-conversion source. However, the photon-number-splitting attack we propose will make practical implementations of this scheme insecure since the parametric down-conversion source may occasionally emit multiphoton pairs. We propose a decoy-state method to make these implementations immune to this attack. With this decoy-state method, both the security distance and key bit rate will be increased.

DOI: 10.1103/PhysRevA.77.062326 PACS number(s): 03.67.Dd

I. INTRODUCTION

As a combination of quantum mechanics and conventional cryptography, the quantum key distribution (QKD) [1–3] can help two distant peers (Alice and Bob) share a secret string of bits, called a key. Unlike conventional cryptography whose security is based on computational complexity, the security of the QKD relies on the fundamental laws of quantum mechanics. Any eavesdropping attempt on an ideal QKD process will introduce an abnormal high bit error rate of the key. By comparing subsets of the key, Alice and Bob can catch any eavesdropping attempt. Polarization and phase time of photons are the most common coding methods to implement the QKD. But birefringence in optical fibers may depolarize the photons, which makes the polarization coding unsuitable for a QKD based on fiber. Phase time coding is commonly used for fiber QKD. Using "plug and play" [3] or Faraday-Michelson interferometers [11], phase time coding can be free from polarization fluctuations due to the birefringence of optical fiber. However, plug and play may be vulnerable to a Trojan attack. And for Faraday-Michelson interferometers [11], it is very sensitive to phase fluctuations from arms between Alice's and Bob's interferometers. To overcome this problem, active compensation, which makes the system more complicated and inefficient, is used.

Alternatively, Walton *et al.* [4] proposed a QKD protocol based on decoherence-free space (DFS) and Boileau *et al.* [5] developed this scheme to use time bins and polarization for encoding. In the scheme of Boileau *et al.*, Alice can encode her qubit in the two-photon states as follows: $|H\rangle|V\rangle$, $|V\rangle|H\rangle$, $(|H\rangle|V\rangle+|V\rangle|H\rangle)/\sqrt{2}$, and $(|H\rangle|V\rangle-|V\rangle|H\rangle/\sqrt{2}$ [in an experiment by Chen *et al.* [6], the four states are $(|H\rangle|V\rangle+|V\rangle|H\rangle)/\sqrt{2}$, $(|H\rangle|V\rangle-|V\rangle|H\rangle)/\sqrt{2}$, $(|H\rangle|V\rangle+i|V\rangle|H\rangle)/\sqrt{2}$, and $(|H\rangle|V\rangle-i|V\rangle|H\rangle/\sqrt{2})$], where H (V) means the horizontal (vertical) polarization mode of photons. The two photons are distinguishable by a fixed time delay Δt_p, which is known to Alice and Bob. Then Alice applies a time delay operation to the V photons, and before Bob detects the two photons, he applies the same time delay operation to the H photons. Finally, Bob detects the two photons in the $|H\rangle|V\rangle$ and $|V\rangle|H\rangle$ bases or $\frac{1}{\sqrt{2}}(|H\rangle|V\rangle+|V\rangle|H\rangle)$, $\frac{1}{\sqrt{2}}(|H\rangle|V\rangle-|V\rangle|H\rangle$ bases. Due to the fact that $|\psi^-\rangle=\frac{1}{\sqrt{2}}(|H\rangle|V\rangle-|V\rangle|H\rangle)$ is invariant under collective unitary transformation, this scheme is insensitive to phase fluctuations from Alice's and Bob's interferometers. If the interval of the time between the two photons is just Δt_p, Bob will successfully get Alice's qubit and this probability will be 2/3 assuming the collective noise is totally random. Besides this, photons from the same pair can provide precise time references for each other. So, in this scheme, an accurate synchronization clock is unnecessary.

Bennett-Brassard 1984 (BB84) type QKD protocols, which are the most-widely used QKD protocols, need a single-photon source, which is not practical with the present technology. Usually, real-file QKD setups [7–11] use attenuated laser pulses (weak coherent states) instead. It means the laser source is equivalent to one that emits n-photon states $|n\rangle$ with probability $P_n=\frac{\mu^n}{n!}e^{-\mu}$, where μ is the average photon number of attenuated lased pulses. This photon-number Poisson distribution stems from the coherent state $|\sqrt{\mu}e^{i\theta}\rangle$ of the laser pulse. Therefore, a few multiphoton events in the laser pulses emitted from Alice open the door to a photon-number-splitting attack (PNS attack) [12–14], which makes the whole QKD process insecure. Fortunately, decoy-state QKD theory [15–18,26], as a good solution to beat PNS attacks, has been proposed. And some prototypes of the decoy-state QKD have been implemented [19–25]. The key point of the decoy-state QKD is to calculate the lower bound of the counting rate of single-photon pulses (S_1^L) and upper bound of the quantum bit error rate (QBER) of bits generated by single-photon pulses (e_1^U). Many methods to improve the performance of the decoy-state QKD have been presented, including more decoy states [26] and a nonorthogonal decoy-state method [27], photon-number-resolving method [28], herald single-photon source method [29,30], and modified coherent-state source method [31]. And for the intensity fluctuations of the laser pulses, Refs. [34] and [35] give good solutions.

As a BB84-type protocol, the scheme of Boileau *et al.* is still vulnerable to PNS attack. This problem will be discussed in details in Sec. II, in which we propose a type of PNS attack. In Sec. III, we propose a decoy-state method to

*Author to whom correspondence should be addressed. zwzhou@ustc.edu.cn
†zfhan@ustc.edu.cn

overcome this problem. In Sec. IV, a numerical simulation will be given. Finally, we will give a summary to end this paper.

II. PNS ATTACK IN THE SCHEME OF BOILEAU *et al.*

To implement the scheme of Boileau *et al.*, an ideal two-photon states source that is far in advance of present technology is needed. In practice, two-photon states are generated by a parametric down-conversion source (PDCS), which will emit n-photon $(n>1)$ pairs with certain probability. However, the state from a type-II PDCS can be written as [32]

$$|\psi\rangle = (\cosh \chi)^{-2} \sum_{n=0}^{\infty} \sqrt{n+1} e^{in\theta} \tanh^n \chi |\Phi_n\rangle, \tag{1}$$

in which $|\Phi_n\rangle$ is the state of an n-photon pair, given by

$$|\Phi_n\rangle = \frac{1}{\sqrt{n+1}} \sum_{m=0}^{n} (-1)^m |n-m,m\rangle_a |m,n-m\rangle_b. \tag{2}$$

Here, $|n,m\rangle_{a(b)} = |H\rangle_{a(b)}^{\otimes n} |V\rangle_{a(b)}^{\otimes m}$, where a and b are two spatial output modes of the PDCS, respectively. By randomizing the phase θ [15], we can write the density matrix of the PDCS as $\rho_\lambda = \int [d\theta/(2\pi)] |\psi\rangle\langle\psi| = P_n(\lambda) |\Phi_n\rangle\langle\Phi_n|$, where, $P_n(\lambda) = (n+1)\lambda^n/(1+\lambda)^{n+2}$, $\lambda = \sinh^2 \chi$, which is half of the average number of photon pairs generated by one pumping pulse and could be adjusted by the intensity of the pumping pulse. Therefore, the PDCS is really just a photon-number-state source emitting n-photon pairs $|\Phi_n\rangle$ with probability $P_n(\lambda)$. For implementations that do not apply phase randomization, Eve may attack this QKD system more powerfully [36]. Therefore, for simplicity we assume that Alice has applied phase randomization to her photon pairs.

Here we focus on the attack on two-photon pairs, because two-photon pairs are dominant among multiphoton pairs. For the practical implementation [6] by Chen *et al.*, Alice delays the b mode of the two spatial outputs of the PDCS with Δt_p. Then through phase-modulation by Pockel cells [6] two-photon pair states can be described in creation operator form as

$$\begin{aligned}
|-\rangle &= \frac{1}{2\sqrt{3}} (H_a^{\dagger 2} V_b^{\dagger 2} - 2 H_a^\dagger V_a^\dagger H_b^\dagger V_b^\dagger + V_a^{\dagger 2} H_b^{\dagger 2}) |\text{vacuum}\rangle, \\
|+\rangle &= \frac{1}{2\sqrt{3}} (H_a^{\dagger 2} V_b^{\dagger 2} + 2 H_a^\dagger V_a^\dagger H_b^\dagger V_b^\dagger + V_a^{\dagger 2} H_b^{\dagger 2}) |\text{vacuum}\rangle, \\
|0\rangle &= \frac{1}{2\sqrt{3}} (H_a^{\dagger 2} V_b^{\dagger 2} + 2i H_a^\dagger V_a^\dagger H_b^\dagger V_b^\dagger - V_a^{\dagger 2} H_b^{\dagger 2}) |\text{vacuum}\rangle, \\
|1\rangle &= \frac{1}{2\sqrt{3}} (H_a^{\dagger 2} V_b^{\dagger 2} - 2i H_a^\dagger V_a^\dagger H_b^\dagger V_b^\dagger - V_a^{\dagger 2} H_b^{\dagger 2}) |\text{vacuum}\rangle,
\end{aligned} \tag{3}$$

where $H_a^\dagger$, $H_b^\dagger$, $V_a^\dagger$, and $V_b^\dagger$ represent the creation operators for horizontal polarized photons in the a mode, horizontal polarized photons in the b mode, vertical polarized photons in the a mode, and vertical polarized photons in the b mode, respectively. For simplicity, we assume Eve adds a beam splitter (BS) to both modes a and b and we name the two spatial modes of the output of the BS as 1 and 2. Now Eve has four spatial-temporal modes $a1$, $a2$, $b1$, and $b2$, and creator operators for horizontal-polarized and vertical-polarized photons in these new modes are correlated with modes a and b by $H_a^\dagger = (1/\sqrt{2})(H_{a1}^\dagger - H_{a2}^\dagger)$, $V_a^\dagger = (1/\sqrt{2})(V_{a1}^\dagger - V_{a2}^\dagger)$, $H_b^\dagger = (1/\sqrt{2})(H_{b1}^\dagger - H_{b2}^\dagger)$, and $V_b^\dagger = (1/\sqrt{2})(V_{b1}^\dagger - V_{b2}^\dagger)$. Then Eve can post-select the states that each of modes $a1$, $b1$, $a2$, and $b2$ has one and only one photon, respectively. We should notice that although through just one BS the probability of success of this post-selection is just 1/4, Eve may use many BSs to make sure that this probability will be close to 1. And states $|-\rangle$, $|+\rangle$, $|0\rangle$, and $|1\rangle$ will be transformed into

$$\begin{aligned}
|-\rangle' &= \frac{1}{2\sqrt{2}} [(H_{a1}V_{b1} - V_{a1}H_{b1})(H_{a2}V_{b2} - V_{a2}H_{b2}) \\
&\quad + (H_{a1}V_{b2} - V_{a1}H_{b2})(H_{a2}V_{b1} - V_{a2}H_{b1})], \\
|+\rangle' &= \frac{1}{2\sqrt{2}} [(H_{a1}V_{b1} + V_{a1}H_{b1})(H_{a2}V_{b2} + V_{a2}H_{b2}) \\
&\quad + (H_{a1}V_{b2} + V_{a1}H_{b2})(H_{a2}V_{b1} + V_{a2}H_{b1})], \\
|0\rangle' &= \frac{1}{2\sqrt{2}} [(H_{a1}V_{b1} + iV_{a1}H_{b1})(H_{a2}V_{b2} + iV_{a2}H_{b2}) \\
&\quad + (H_{a1}V_{b2} + iV_{a1}H_{b2})(H_{a2}V_{b1} + iV_{a2}H_{b1})], \\
|1\rangle' &= \frac{1}{2\sqrt{2}} [(H_{a1}V_{b1} - iV_{a1}H_{b1})(H_{a2}V_{b2} - iV_{a2}H_{b2}) \\
&\quad + (H_{a1}V_{b2} - iV_{a1}H_{b2})(H_{a2}V_{b1} - iV_{a2}H_{b1})],
\end{aligned} \tag{4}$$

where $H(V)_X$ represents state vector $|H(V)\rangle_X$ for abbreviation and the same below. Then Eve could use a unitary transformation $\mathcal{U}_1$ to the photons in modes $a1$ and $b2$. The definition of $\mathcal{U}_1$ is given by $\mathcal{U}_1 HVE_0 = HVE_1$, $\mathcal{U}_1 VHE_0 = VHE_1$, $\mathcal{U}_1 HHE_0 = HHE_2$, and $\mathcal{U}_1 VVE_0 = VVE_2$, in which E_x is an assist state of Eve satisfying $\langle E_0|E_1\rangle = \langle E_0|E_2\rangle = \langle E_1|E_2\rangle = 0$. Eve post-selects E_1 through projection $P_1 = |E_1\rangle\langle E_1|$ and then the four states will be mapped onto the states below with probability 75%:

$$\begin{aligned}
|-\rangle'' &= \frac{1}{\sqrt{5}} (2|X\rangle - |Y\rangle), \\
|+\rangle'' &= \frac{1}{\sqrt{5}} (2|X\rangle + |Y\rangle), \\
|0\rangle'' &= \frac{1}{\sqrt{5}} (2|X'\rangle + i|Y\rangle),
\end{aligned}$$

$$|1\rangle'' = \frac{1}{\sqrt{5}}(2|X'\rangle + i|Y\rangle), \tag{5}$$

where $|X\rangle = (1/\sqrt{2})(H_{a1}V_{b1}H_{a2}V_{b2} + V_{a1}H_{b1}V_{a2}H_{b2})$, $|Y\rangle = (1/\sqrt{2})(H_{a1}H_{b1}V_{a2}V_{b2} + V_{a1}V_{b1}H_{a2}H_{b2})$, and $|X'\rangle = (1/\sqrt{2})(H_{a1}V_{b1}H_{a2}V_{b2} - V_{a1}H_{b1}V_{a2}H_{b2})$. Now, Eve can construct another unitary transformation $\mathcal{U}_2$ defined by $\mathcal{U}_2|X\rangle|E_0\rangle = (\sqrt{3}|Z\rangle|E_1\rangle + |X\rangle|E_2\rangle)/2$, $\mathcal{U}_2|X'\rangle|E_0\rangle = (\sqrt{3}|Z\rangle|E_3\rangle + |X'\rangle|E_2\rangle)/2$, and $\mathcal{U}_2|Y\rangle|E_0\rangle = |Y\rangle|E_2\rangle$. Here, $|E\rangle$ represents an assist states of Eve and $\langle E_0|E_1\rangle = \langle E_0|E_2\rangle = \langle E_1|E_2\rangle = 0$. And $|Z\rangle$ is any state of photons in modes $a1$, $b1$, $a2$, and $b2$. With $\mathcal{U}_2$ and projection operation $P_2 = |E_2\rangle\langle E_2|$, the four photon states will be mapped onto the following form with probability 40%:

$$|-\rangle''' = \frac{1}{\sqrt{2}}(|X\rangle - |Y\rangle) = \frac{1}{\sqrt{2}}(H_{a1}V_{b2} - V_{a1}H_{b2})\frac{1}{\sqrt{2}}(H_{a2}V_{b1} - V_{a2}H_{b1}),$$

$$|+\rangle''' = \frac{1}{\sqrt{2}}(|X\rangle + |Y\rangle) = \frac{1}{\sqrt{2}}(H_{a1}V_{b2} + V_{a1}H_{b2})\frac{1}{\sqrt{2}}(H_{a2}V_{b1} + V_{a2}H_{b1}),$$

$$|0\rangle''' = \frac{1}{\sqrt{2}}(|X\rangle + i|Y\rangle) = \frac{1}{\sqrt{2}}(H_{a1}V_{b2} + iV_{a1}H_{b2})\frac{1}{\sqrt{2}}(H_{a2}V_{b1} + iV_{a2}H_{b1}),$$

$$|1\rangle''' = \frac{1}{\sqrt{2}}(|X\rangle - i|Y\rangle) = \frac{1}{\sqrt{2}}(H_{a1}V_{b2} - iV_{a1}H_{b2})\frac{1}{\sqrt{2}}(H_{a2}V_{b1} - iV_{a2}H_{b1}). \tag{6}$$

Obviously, with the states $|-\rangle'''$, $|+\rangle'''$, $|0\rangle'''$, and $|1\rangle'''$, Eve can keep one pair and send the other pair to Bob through a special channel controlled by herself. When Alice and Bob do basis reconciliation, Eve will get all secret information. This is just the same as a PNS attack [12–14].

Let us review our attack strategy. First, Eve divides the two photons modes a and b into modes $a1$, $a2$ and $b1$, $b2$, respectively. With many BSs, the success probability of this step is close to 1. Second, Eve applies the unitary transformation $\mathcal{U}_1$ and projection P_1; she gets an intermediate state with success probability 75%. Finally, she applies the unitary transformation $\mathcal{U}_2$ and projection P_2; she gets the final state from which she can launch a PNS attack immediately and the success probability of this step is 40%. Overall, for two-photon pairs Eve will launch a PNS attack with probability of $75\% \times 40\% = 30\%$ or discard the failure case with probability $100\% - 30\% = 70\%$.

According to the above facts and the discussion of Refs. [12–14], we know that the security distance (L) of this scheme must obey $P_1(\lambda)(10^{-kL/10})^2 \geq P_2(\lambda) \times 30\%$, in which k is the transmission fiber loss constant. If we assume $k = 0.2$ dB/km, which is a typical value of this constant, and $\lambda = 0.1$, we obtain $L \leqq 37.4$ km. This is a highly unsatisfactory situation. How to prolong the security distance is what we will discuss in the next section.

III. DECOY STATES OF THE SCHEME OF BOILEAU *et al.*

The rate of secret key bits (R) for the BB84 protocol with nonideal source can be determined from Ref. [33]:

$$R \geq R^L = q\{-Q_\lambda f(E_\lambda)H_2(E_\lambda) + P_1(\lambda)S_1^L[1 - H_2(e_1^U)]\}. \tag{7}$$

Here, R^L represents the lower bound of R, q depends on protocol (1/2 for the scheme of Boileau *et al.*), Q_λ is the overall counting rate for the photon pairs, λ is half of the average number of the photon pairs, $f(E_\lambda)$ is the error correction efficiency, E_λ is the QBER of the key bit, H_2 is the binary Shannon information function, S_1 is the counting rate for the one-photon pairs, and e_1 is the QBER of the key bits generated by the one-photon pairs. Similar to the BB84 protocol based on weak coherent states, we need to modulate λ to several values randomly. Through watching counting rates for different λ, we can obtain the lower bound of S_1 (S_1^L) and the upper bound of e_1 (e_1^U). Finally, R^L can be obtained from Eq. (7).

Our three-intensity protocol is the following: Alice randomly emits photon pairs of density matrices ρ_λ, $\rho_{\lambda'}$, and 0 [λ for signal states, λ' ($\lambda > \lambda'$), and 0 for decoy states]; then, Bob can obtain their counting rates Q_λ, $Q_{\lambda'}$, and S_0. With formulas we derive later, S_1^L and e_1^U can be obtained. Finally, R^L is given by Eq. (7). Now we derive these formulas.

The counting rates for the two intensity (λ and λ') photon pairs are determined by

$$Q_\lambda = \sum_{n=0}^{\infty} P_n(\lambda)S_n, \tag{8}$$

$$Q_{\lambda'} = \sum_{n=0}^{\infty} P_n(\lambda')S_n, \tag{9}$$

where S_n represents the counting rate for n-photon pair states $|\Phi_n\rangle$. Then the QBER for the λ (E_λ) is determined by

$$E_\lambda Q_\lambda = \sum_{n=0}^{\infty} e_n P_n(\lambda)S_n, \tag{10}$$

in which e_n is the QBER of the key bits generated by the n-photon pairs $|\Phi_n\rangle$. Before the derivation of the formula to calculate S_1^L and e_1^U, we prove that $\frac{P_2(\lambda)}{P_2(\lambda')}P_n(\lambda') \leq P_n(\lambda)$ for all $n \geq 2$:

$$\frac{P_2(\lambda)}{P_n(\lambda)} - \frac{P_2(\lambda')}{P_n(\lambda')} = \frac{3}{n+1}\left[\left(1 + \frac{1}{\lambda}\right)^{n-2} - \left(1 + \frac{1}{\lambda'}\right)^{n-2}\right] \leq 0. \tag{11}$$

With this result, we can deduce the formula for calculating S_1^L:

$$Q_\lambda = P_0(\lambda)S_0 + P_1(\lambda)S_1 + P_2(\lambda)S_2 + P_3(\lambda)S_3 + \cdots$$
$$\geq P_0(\lambda)S_0 + P_1(\lambda)S_1 + \frac{P_2(\lambda)}{P_2(\lambda')}\sum_{n=2}^{\infty} P_n(\lambda')S_n. \quad (12)$$

With Eq. (9), we have

$$S_1^L = \frac{[P_2(\lambda')P_0(\lambda) - P_2(\lambda)P_0(\lambda')]S_0 + P_2(\lambda)Q_{\lambda'} - P_2(\lambda')Q_\lambda}{P_2(\lambda)P_1(\lambda') - P_2(\lambda')P_1(\lambda)}. \quad (13)$$

According to Eq. (10) and [18], e_1^U can be given by

$$e_1^U = \frac{E_\lambda Q_\lambda - S_0 P_0(\lambda)/2}{P_1(\lambda)S_1^L}. \quad (14)$$

With Eqs. (13) and (14), S_1^L and e_1^U can be obtained. Finally, R^L is given by Eq. (7).

For the experiment, the two-intensity decoy-state protocol is quite convenient [25]. In this case, Alice randomly emits photon pairs of density matrix ρ_λ for signal states and $\rho_{\lambda'}$ for decoy states; then, Bob can obtain their counting rates Q_λ and $Q_{\lambda'}$. We now deduce the formula to calculate S_1^L and e_1^U just from Q_λ and $Q_{\lambda'}$.

According to Eq. (10), the upper bound of S_0 (S_0^U) can be given by

$$S_0^U = \frac{2E_\lambda Q_\lambda}{P_0(\lambda)}. \quad (15)$$

Then, from Eq. (10), S_1^L for the two-intensity case can be given by

$$S_1^L = \frac{2[P_2(\lambda')P_0(\lambda) - P_2(\lambda)P_0(\lambda')]\frac{E_\lambda Q_\lambda}{P_0(\lambda)} + P_2(\lambda)Q_{\lambda'} - P_2(\lambda')Q_\lambda}{[P_2(\lambda)P_1(\lambda') - P_2(\lambda')P_1(\lambda)]P_0(\lambda)}. \quad (16)$$

To get e_1^U for the two-intensity case, we just set the lower bound of S_0 (S_0^L) to 0; then, with Eqs. (10) and (16), e_1^U is given by

$$e_1^U = \frac{E_\lambda Q_\lambda}{P_1(\lambda)S_1^L}. \quad (17)$$

Equations (16) and (17) are for the two-intensity case. With these equations, we have established the basic methods to beat the PNS attack in the QKD scheme of Boileau *et al.* Next, we will make sure that this decoy-state method can improve the performance of the QKD scheme of Boileau *et al.* impressively.

IV. IMPROVEMENT BY DECOY STATES

Now, we will show the improvement for the performance by the introduction of decoy states through numerical simulations. In the following discussions and simulations, we neglect the error induced by channels and assume Bob's measurements are perfect except for a few dark counts for simplicity. According to Ref. [6], Bob's measurement is equivalent to the projection onto the polarization states F and S defined by $H=(F+S)/\sqrt{2}$ and $V=(F-S)/\sqrt{2}$, respectively. We rewrite the encoding states $|+\rangle$ and $|-\rangle$ in the form of F and S: $|+\rangle=\frac{1}{\sqrt{n+1}}\Sigma_{m=0}^{n}(-1)^m F_a^{n-m}S_a^m F_b^{n-m}S_a^m$ and $|-\rangle=\frac{1}{\sqrt{n+1}}\Sigma_{m=0}^{n}(-1)^m F_a^{n-m}S_a^m F_b^m S_a^{n-m}$. For Bob, if he observes F_aS_b or S_aF_b, it will be $|+\rangle$, while F_aF_b or S_aS_b is for the result of $|+\rangle$. According to Ref. [18], the transmission efficiency for n-photon pulses, η_n, can be written as $\eta_n=1-(1-\eta)^n$, in which η is the transmission efficiency of the fiber channel and $\eta=10^{(-kL/10)}$, K is the transmission fiber loss constance, and L is the fiber length. Since our goal is to show the difference between the original QKD scheme of Boileau *et al.* and this scheme with decoy states, but not exact R^L versus fiber length, we take the efficiency of the detector and loss due to projection onto the DFS space or other causes just as a part of fiber loss and do not concern ourselves with these values. We assume that dark counting rate of the detectors is D. Since Bob must neglect all the three or fourfold counts, S_n can be written as

$$S_n = \frac{(1-D)^2}{n+1}\sum_{m=0}^{n}\{[\eta_{n-m}(1-\eta)^m + \eta_m(1-\eta)^{n-m}]^2\}$$
$$+ 4\eta_{n-m}(1-\eta)^m(1-\eta)^n D + 4\eta_m(1-\eta)^{n-m}(1-\eta)^n D$$
$$+ 4(1-\eta)^{2n}D^2. \quad (18)$$

Then with Eq. (8), we can obtain formulas to estimate Q_λ and $Q_{\lambda'}$:

$$Q_\lambda = \sum_{n=0}^{\infty} P_n(\lambda)S_n$$
$$= \frac{2(1-D)^2}{[1+\lambda\eta(3-\eta)+\lambda^2\eta^2(2-\eta)]^2}$$
$$\times\{4\lambda\eta D(1-\eta)(1+\lambda\eta) + 2D^2(1+\lambda\eta)^2$$
$$+ \lambda\eta^2[1+\lambda^2(2-\eta)\eta + \lambda(\eta^2 - 2\eta + 3)]\}. \quad (19)$$

For simplicity we neglect the probability of a surviving photon hitting the wrong detector; then, e_n is written as

$$e_n S_n = \left[\sum_{m=0}^{n} (2\eta_{n-m}(1-\eta)^m(1-\eta)^{n-m}\eta_m + 2\eta_m(1-\eta)^{n-m}(1-\eta)^n D + 2\eta_{n-m}(1-\eta)^m(1-\eta)^n D + 2(1-\eta)^{2n} D) \right] \frac{(1-D)^2}{n+1}, \quad (20)$$

in which the first term of the summation corresponds to the case of the photons in modes a and b both hitting the detectors. Only when $n \geq 2$ is this term not equal to 0. The second and third terms in the above summation represent the case of photons in only one mode (a or b) hitting the detector. The dark count of one detector may result in the QBER in this situation. The last term of the summation is for the case of all photons being absorbed by fiber.

With this, we can estimate the QBER E_λ as

$$E_\lambda = \sum_{n=0}^{\infty} P_n(\lambda) e_n S_n / Q_\lambda = [D + \lambda D\eta + \lambda\eta(1-\eta)]^2 \times \{[4\lambda D\eta(1-\eta)(1+\lambda\eta) + 2D^2(1+\lambda\eta)^2 + \lambda\eta^2(1+\lambda^2\eta(2-\eta) + \lambda(\eta^2 - 2\eta + 3))]\}^{-1}. \quad (21)$$

Now with Eqs. (19) and (21) and setting $k=0.2$ dB/km, $D=10^{-6}$/pulse, and $f(E_\lambda)=1.2$, Q_λ, $Q_{\lambda'}$, and E_λ can be calculated by numerical simulations. Then, with Eqs. (13) and (14), S_1^L and e_1^U can be obtained. Finally, the relation between R^L and the fiber length L can be acquired. The results are depicted in Fig. 1. In Fig. 1, the solid curve is for the case that no decoy state is employed. In this case, for the calculation of S_1^L and e_1^U we have to assume that $S_n=1$ ($n \geq 2$) and with Eq. (15), then obviously S_1 is given by

$$S_1^L = \frac{Q_\lambda - P_0(\lambda)S_0^U - \sum_{n=2}^{\infty} P_2(\lambda)}{P_1(\lambda)} = \frac{Q_\lambda(1-2E_\lambda) - [1 - P_0(\lambda) - P_1(\lambda)]}{P_1(\lambda)}. \quad (22)$$

Then e_1^U is calculated by Eq. (14). With this method, R^L is obtained from Eq. (7). From Fig. 1, we found that the three-intensity decoy-state method can improve the performance of the scheme of Boileau *et al.* dramatically. The longest security distance in the original scheme of Boileau *et al.* is about 18 km, while this distance for the three-intensity decoy-state method will be 40 km. This improvement means about a 4.4-dB increase in the longest security distance.

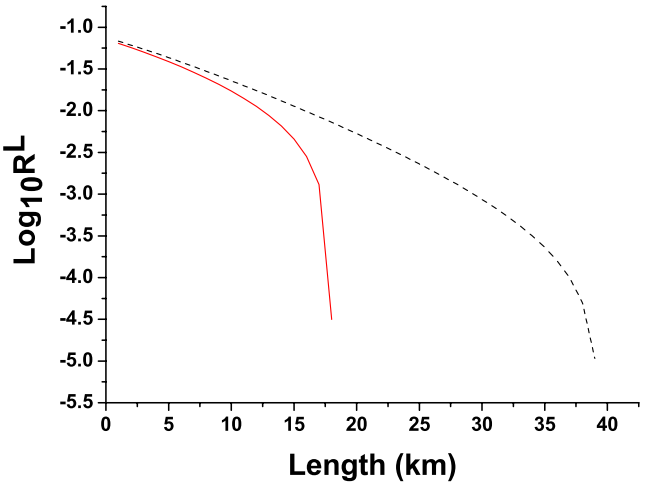

FIG. 1. (Color online) Lower bound of the secret bit generation rate (R_1^L) versus fiber length L. Solid curve: no decoy states is employed. Alice just emits a PDCS with a half average number of photon pairs, $\lambda=0.1$. Dashed curve: the three-intensity case. Alice randomly used a PDCS with a half average number of photon pairs, $\lambda=0.1$, $\lambda'=0.01$, and 0.

V. CONCLUSION

According to above discussions, we proved that through the introduction of the decoy-state method, especially the three-intensity decoy states, the performance of the DFS-type QKD of Boileau *et al.* would be dramatically improved. Because of the three-intensity decoy-state protocol, the increase of the longest security distance can be 4.4 dB. This increase relies on the ability of the three-intensity decoy-state protocol to obtain a tighter bound of S_1^L and e_1^U. Furthermore, one can estimate the information leaked to Eve with high precision and a higher key bit rate and a longer security distance can be obtained. We hope that our protocol can be implemented soon.

ACKNOWLEDGMENTS

This work was supported by National Fundamental Research Program of China (Grant No. 2006CB921900), National Natural Science Foundation of China (Grants No. 60537020 and No. 60621064), and the Innovation Funds of the Chinese Academy of Sciences.

[1] C. H. Bennett and G. Brassard, in *Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing, Bangalore, India* (IEEE, New York, 1984), pp. 175–179.
[2] A. K. Ekert, Phys. Rev. Lett. **67**, 661 (1991).
[3] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Rev. Mod. Phys. **74**, 145 (2002).
[4] Z. D. Walton, A. F. Abouraddy, A. V. Sergienko, B. E. A. Saleh, and M. C. Teich, Phys. Rev. Lett. **91**, 087901 (2003).
[5] J.-C. Boileau, R. Laflamme, M. Laforest, and C. R. Myers, Phys. Rev. Lett. **93**, 220501 (2004).
[6] Teng-Yun Chen, Jun Zhang, J.-C. Boileau, Xian-Min Jin, Bin

Yang, Qiang Zhang, Tao Yang, R. Laflamme, and Jian-Wei Pan, Phys. Rev. Lett. **96**, 150504 (2006).
[7] M. Bourennane *et al.*, Opt. Express **4**, 383 (1999).
[8] D. Stucki *et al.*, New J. Phys. **4**, 41 (2002).
[9] H. Kosaka *et al.*, Electron. Lett. **39**, 1199 (2003).
[10] C. Gobby, Z. L. Yuan, and A. J. Shields, Appl. Phys. Lett. **84**, 3762 (2004).
[11] X.-F. Mo *et al.*, Opt. Lett. **30**, 2632 (2005).
[12] B. Huttner, N. Imoto, N. Gisin, and T. Mor, Phys. Rev. A **51**, 1863 (1995).
[13] G. Brassard, N. Lütkenhaus, T. Mor, and B. C. Sanders, Phys. Rev. Lett. **85**, 1330 (2000).
[14] N. Lütkenhaus, Phys. Rev. A **61**, 052304 (2000).
[15] W.-Y. Hwang, Phys. Rev. Lett. **91**, 057901 (2003).
[16] H.-K. Lo, X. Ma, and K. Chen, Phys. Rev. Lett. **94**, 230504 (2005).
[17] X.-B. Wang, Phys. Rev. Lett. **94**, 230503 (2005).
[18] X. Ma, B. Qi, Y. Zhao, and H.-K. Lo, Phys. Rev. A **72**, 012326 (2005).
[19] Y. Zhao, B. Qi, X. Ma, H.-K. Lo, and L. Qian, Phys. Rev. Lett. **96**, 070502 (2006).
[20] Yi Zhao *et al.*, in *Proceedings of IEEE International Symposium on Information Theory, Seattle, Washington, USA* (IEEE, New York, 2006), pp. 2094–2098.
[21] C.-Z. Peng, J. Zhang, D. Yang, W.-B. Gao, H.-X. Ma, H. Yin, H.-P. Zeng, T. Yang, X.-B. Wang, and J.-W. Pan, Phys. Rev. Lett. **98**, 010505 (2007).
[22] D. Rosenberg, J. W. Harrington, P. R. Rice, P. A. Hiskett, C. G. Peterson, R. J. Hughes, A. E. Lita, S. W. Nam, and J. E. Nordholt, Phys. Rev. Lett. **98**, 010503 (2007).
[23] Z. L. Yuan, A. W. Sharpe, and A. J. Shields, Appl. Phys. Lett. **90**, 011118 (2007).
[24] Tobias Schmitt-Manderbach *et al.*, Phys. Rev. Lett. **98**, 010504 (2007).
[25] Z.-Q. Yin *et al.*, e-print arXiv:quant-ph/0704.2941.
[26] X.-B. Wang, Phys. Rev. A **72**, 012322 (2005).
[27] J.-B. Li and X.-M. Fang, Chin. Phys. Lett. **23**, 775 (2006).
[28] Qing-yu Cai and Yong-gang Tan, Phys. Rev. A **73**, 032305 (2006).
[29] Tomoyuki Horikiri and Takayoshi Kobayashi, Phys. Rev. A **73**, 032331 (2006).
[30] Qin Wang, X.-B. Wang, and G.-C. Guo, Phys. Rev. A **75**, 012312 (2007).
[31] Z.-Q. Yin, Z.-F. Han, F.-W. Sun, and G.-C. Guo, Phys. Rev. A **76**, 014304 (2007).
[32] X. Ma, C.-H. F. Fung, and H.-K. Lo, Phys. Rev. A **76**, 012307 (2007).
[33] D. Gottesman, H.-K. Lo, N. Lütkenhaus, and J. Preskill, Quantum Inf. Comput. **4**, 325 (2004).
[34] X.-B. Wang, C.-Z. Peng, and J.-W. Pan, Appl. Phys. Lett. **90**, 031110 (2007).
[35] X.-B. Wang, Phys. Rev. A **75**, 052301 (2007).
[36] Hoi-Kwong Lo and John Preskill, e-print arXiv:quant-ph/0504209.