State-discrimination attack on discretely modulated continuous-variable quantum key distribution

Peng Huang,[*] Jian Fang,[†] and Guihua Zeng[‡]
State Key Laboratory of Advanced Optical Communication Systems and Networks, Shanghai Key Laboratory of Intelligent Sensing and Recognition, Shanghai Jiaotong University, Shanghai 200240, China

(Received 19 December 2013; published 28 April 2014)

The continuous-variable quantum key distribution (CVQKD) schemes with discrete modulation are proposed to allow distributions of secret keys over long distance due to the sharing of discrete data. However, the nonorthogonal signal states in these schemes can be discriminated by using quantum receivers with low error rates, which may incur state-discrimination (SD) attacks. We consider the feasibility of Eve's attacks on discrete-modulated CVQKD protocol based on the SD receiver. In particular, an intercept-resend attack is proposed on the four-state protocol based on an SD receiver and a heralded noiseless linear amplifier. The security analysis shows that the secret key rate inferred by Alice and Bob can be larger than its true value, which reveals that the original four-state protocol is not secure under the SD attack. Fortunately, the decoy states can be well applied to remedy this defect, but with the cost of complicated practical implementation.

DOI: 10.1103/PhysRevA.89.042330 PACS number(s): 03.67.Dd, 42.50.−p

I. INTRODUCTION

Continuous-variable quantum key distribution (CVQKD) [1–7] provides another way to allow two distant parties, the sender Alice and the receiver Bob, to establish a secret key through insecure quantum and classical channels. In CVQKD protocols, Alice usually encodes information in the quadratures of an optical field with Gaussian modulation, and Bob can decode the secret information with high-efficiency homodyne or heterodyne detection. So far, the CVQKD protocols have been proved secure against general collective attacks [8–10] and coherent attacks asymptotically based on the quantum de Finetti theorem [11]. And recently, these protocols were further proved to be secure against general coherent attacks in the finite-size regime by employing a postselection technique [12] and an entropic uncertainty relation [13], respectively.

However, the secure distances of CVQKD are short in contrast to discrete-variable quantum key distribution (DVQKD) [1,14,15]. The main reason is that the distributed raw key data between Alice and Bob in CVQKD schemes are usually Gaussian random values, where the classical postprocessing of continuous data is much more complicated than the discrete counterpart. To solve this main problem, several solutions are proposed, such as designing a reconciliation code with high efficiency even at low signal-to-noise ratio (SNR) [16,17], and using a noiseless linear amplifier (NLA) [18] or photon substraction operation [19]. In particular, it has been shown that discretely modulated schemes, such as the four-state protocol [20], may extremely improve the secure transmission distances, since there exist error correction codes with high efficiency for discrete values even at very low SNR. It should be mentioned that the unconditional security proof of the four-state protocol [20] relies on a hidden assumption that the quantum channel is linear. To remove this assumption, an improved protocol with decoy states is proposed in [21].

In discretely modulated protocols, Alice encodes the key information on the phase of some nonorthogonal coherent states, and Bob uses homodyne detection to obtain the values of related quadratures to extract the discrete key information. On the other hand, the discretely modulated information can be detected by using a quantum receiver which discriminates the multiple nonorthogonal coherent states. Recently, some theoretical and experimental strategies have been proposed to implement the state-discrimination (SD) receiver so that the nonorthogonal phase states can be discriminated with error rates below the standard quantum limit (SQL) [22–24], which is referred to as the limit of perfect homodyne detection. It implies that when legitimate parties communicate by using the discretely modulated CVQKD protocol, the secret key encoded on the phases of the signal states may be subject to eavesdropping by Eve when she uses the SD receiver.

In this paper, we investigate the security of the four-state CVQKD protocol proposed in [20] under Eve's SD attacks. Specifically, we consider that Eve performs a simple eavesdropping strategy, i.e., intercept-resend attack, based on a SD receiver and a heralded NLA [25–31]. In principle, the error rate to discriminate the four nonorthogonal states decreases with the amplitude of the states, and a probabilistic NLA can well amplify the amplitude of a coherent state without introducing extra noise. Thus, the use of NLA can dramatically decrease the error probability of Eve's SD receiver and enhance the attack. Security analysis shows that Eve can capture more secret information through the proposed SD attack than the counterpart evaluated from the shared data by legitimate parties. It should be mentioned here that this attack strategy might not be optimal, but, as revealed below, the original four-state CVQKD protocol will be not secure under this attack.

This paper is organized as follows. In Sec. II, we first introduce the discretely modulated CVQKD protocols, in particular the four-state protocol, and then propose an SD attack on the four-state CVQKD protocol. In Sec. III, we analyze the security of the original four-state protocol under

[*] huang.peng@sjtu.edu.cn
[†] jian.fang.sh@gmail.com
[‡] ghzeng@sjtu.edu.cn

the proposed SD attack, and then in Sec. IV we discuss the security of the improved four-state protocol with decoy states under the SD attack. Finally, conclusions are drawn in Section V.

II. SD ATTACKS IN DISCRETELY MODULATED CVQKD PROTOCOLS

A. The discretely modulated CVQKD protocol

Before introducing the SD attacks for discretely modulated CVQKD protocols, we first take a brief review of the discretely modulated CVQKD protocols. Until now, some types of discretely modulated CVQKD protocols have been proposed, such as the two- and four-state protocols [20,32]. The discretely modulated protocols can be generalized to the one with N coherent states $|\alpha_k\rangle = |\alpha e^{2ik\pi/N}\rangle$ [33], where α is a positive number related to the modulation variance as $V_A = 2\alpha^2$. Without loss of generality, we focus on the discretely modulated protocol with $N = 4$, which corresponds to the four-state protocol [20]. Considering the prepare-and-measure (P&M) version of the four-state protocol, Alice randomly chooses one of the coherent states $|\alpha_k\rangle = |\alpha e^{(2k+1)i\pi/4}\rangle$, $k \in \{0,1,2,3\}$, and sends it to Bob with probability 1/4. So Bob receives a mixture state ρ_4 with the form

$$\rho_4 = \frac{1}{4}\sum_{k=0}^{3} |\alpha_k\rangle\langle\alpha_k|. \tag{1}$$

While in the entanglement-based (EB) version, a purification $|\Psi\rangle$ of this state is used such that $\rho_4 = \mathrm{Tr}_A(|\Psi\rangle\langle\Psi|)$. The state ρ_4 can be diagonalized as

$$\rho_4 = \lambda_0|\phi_0\rangle\langle\phi_0| + \lambda_1|\phi_1\rangle\langle\phi_1| + \lambda_2|\phi_2\rangle\langle\phi_2| + \lambda_3|\phi_3\rangle\langle\phi_3|, \tag{2}$$

where

$$\begin{aligned}\lambda_{0,2} &= \tfrac{1}{2}e^{-\alpha^2}[\cosh(\alpha^2) \pm \cos(\alpha^2)],\\ \lambda_{1,3} &= \tfrac{1}{2}e^{-\alpha^2}[\sinh(\alpha^2) \pm \sin(\alpha^2)].\end{aligned} \tag{3}$$

The pure state $|\Psi\rangle$ is defined as

$$\begin{aligned}|\Psi\rangle &= \sum_{k=0}^{3} \sqrt{\lambda_k}|\phi_k\rangle|\phi_k\rangle,\\ &= \frac{1}{2}\sum_{k=0}^{3} |\psi_k\rangle|\alpha_k\rangle,\end{aligned} \tag{4}$$

where

$$\begin{aligned}|\phi_k\rangle &= \frac{e^{-\alpha^2/2}}{\sqrt{\lambda_k}}\sum_{n=0}^{\infty}(-1)^n \frac{\alpha^{4n+k}}{\sqrt{(4n+k)!}}|4n+k\rangle,\\ |\psi_k\rangle &= \frac{1}{2}\sum_{m=0}^{3} e^{(2k+1)im\pi/4}|\phi_m\rangle\end{aligned} \tag{5}$$

for $k \in \{0,1,2,3\}$, where the states $|\psi_k\rangle$ are orthogonal non-Gaussian states.

The P&M version of the original four-state protocol can be described as follows:

(i) Alice randomly sends one of the coherent states $|\alpha_k\rangle = |\alpha e^{(2k+1)i\pi/4}\rangle, k = 0,1,2,3$, to Bob through a lossy and noisy quantum channel, characterized by a transmission efficiency T and an excess noise ϵ.

(ii) After receiving the states, Bob applies homodyne (or heterodyne) detection to measure randomly one of the two quadratures X or P (or both quadratures). Then Bob reveals its absolute value through the classical authenticated channel and keeps its sign, which encodes the bit of the secret key. Thus, Alice and Bob have shared a string of correlated bits.

(iii) Alice and Bob extract a string of the secret key by using error correction and privacy amplification on the shared binary data.

Also, the equivalent EB version of the four-state protocol can be described as follows:

(a) Alice prepares two-mode entanglement states $|\Psi\rangle$ defined in Eq. (4) and performs projective measurements on half of the states. Then she sends the other half to Bob through the quantum channel.

(b) Bob applies homodyne (or heterodyne) detection to measure one of two quadratures X or P randomly (or both quadratures).

(c) Alice and Bob extract a string of the secret key by using error correction and privacy amplification.

It should be mentioned that the projection measurement $|\psi_k\rangle\langle\psi_k|$ Alice performs in the EB scheme of the four-state protocol only discriminates which coherent state is sent to Bob.

B. SD attacks on four-state CVQKD protocol with NLA

As known in the four-state protocol, Alice prepares four coherent states with four different phases but the same amplitude which is related to the modulation variance. So Eve can apply a quantum receiver to discriminate the four nonorthogonal coherent states with low error probability. The simplest strategy is just the intercept-resend attack based on the SD receiver. As known, an intercept-resend attack by Eve consists in measuring out the quantum signals sent by Alice. Then, Eve prepares the new signal states according to the measurement results and transmits them through a lossless quantum channel to Bob, where the quantum states are reproduced as similarly as possible to the ones sent by Alice. However, this eavesdropping behavior transforms the original quantum channel between Alice and Bob into an entanglement-breaking channel, which will deteriorate the distribution of secret keys between Alice and Bob.

The intercept-resend attack for the four-state protocol based on the SD receiver is depicted in Fig. 1. Eve intercepts all the coherent states $|\alpha_k\rangle, k = 0,1,2,3$ sent by Alice and amplifies the states with a heralded NLA, which can be described as a trace-preserving operation such that

$$\mathcal{T}[|\alpha_k\rangle\langle\alpha_k|] = P_{\mathrm{s}}|g\alpha_k\rangle\langle g\alpha_k| + (1 - P_{\mathrm{s}})|0\rangle\langle 0|, \tag{6}$$

where $g \geqslant 1$ is the gain of amplifier and P_{s} is the success probability. Thus Eve produces an amplified state $|\beta_k\rangle\langle\beta_k| = |g\alpha_k\rangle\langle g\alpha_k|$ with probability P_{s} and simply replaces the state with the vacuum state $|0\rangle\langle 0|$. The success probability of the NLA depends on many experimental factors. Here we consider its upper bound based on very general principles as in [18].

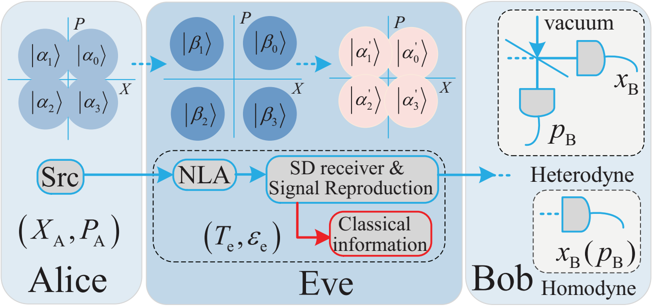

FIG. 1. (Color online) The intercept-resend attack for a four-state protocol based on the SD receiver.

Any trace-preserving quantum operation cannot decrease the fidelity $\mathcal{F}$ between two quantum states [34], that is,

$$\mathcal{F}(|\alpha_k\rangle\langle\alpha_k|, |0\rangle\langle 0|) \leqslant \mathcal{F}(\mathcal{T}[|\alpha_k\rangle\langle\alpha_k|], |0\rangle\langle 0|), \tag{7}$$

which gives an upper bound of P_s. Thus, we find that P_s should verify

$$\langle 0|\alpha_k\rangle\langle\alpha_k|0\rangle \leqslant \langle 0|(P_s|\beta_k\rangle\langle\beta_k| + (1 - P_s)|0\rangle\langle 0|)|0\rangle, \tag{8}$$

which can be simplified as

$$P_s \leqslant \frac{1 - \exp(-|\alpha|^2)}{1 - \exp(-|g\alpha|^2)}. \tag{9}$$

After amplifying the coherent states, Eve performs the SD-receiver-based attack on the output coherent states $|\beta_k\rangle$, $k = 0,1,2,3$, to capture the encoded classical information, i.e., the phases of the states, which reveals the encoded binary secret key. According to the measurement outcomes, Eve reproduces the coherent states $|\alpha_k'\rangle$, $k = 0,1,2,3$, and sends them to Bob with the vacuum states $|0\rangle\langle 0|$ which are produced in the cases of failed implementation of NLA. Also, she substitutes the practical noisy and lossy channel with a better one. Here we consider the case when Eve performs an optimal attack; i.e., she replaces the quantum channel with a perfect one. Since the SD receiver is not perfect, the cases that $|\alpha_k\rangle \neq |\alpha_k'\rangle$ will also introduce excess noise to Bob's side. For critical consideration, we suppose the legitimate party Bob performs perfect homodyne or heterodyne detection.

Different from the general individual and collective attack strategies, Eve directly measures out every signal state sent by Alice, but not the ancillary states interacted by herself. According to the eavesdropping strategy, the key point to successfully implement the intercept-resend attack lies in the SD receiver. As proposed in [22–24], the error probabilities to discriminate the nonorthogonal coherent states in a quadrature phase-shift keying (QPSK) format can be even lower than the theoretical limit of a perfect 100% efficient conventional coherent receiver, i.e., the SQL that defines the minimum average error probability with which the nonorthogonal states can be distinguished by direct measurement of the modulated physical observable of coherent states. The SQL for discrimination of the four amplified nonorthogonal coherent states in the QPSK format is given by

$$P^g_{\mathrm{SQL}} = 1 - \left[1 - \tfrac{1}{2}\mathrm{erfc}\left(\sqrt{|g\alpha|^2/2}\right)\right]^2, \tag{10}$$

where $g\alpha$ is the amplified amplitude and $\mathrm{erfc}(x) = \frac{2}{\sqrt{\pi}}\int_x^\infty e^{-t^2}dt$. Remarkably, quantum mechanics allows for a lower error bound, known as the Helstrom bound [35], which can be approached or achieved by optimized discrimination strategies. The Helstrom bound for the amplified QPSK signals can be well approximated by using the square-root measure (SRM) [36], which is expressed as

$$P^g_{\mathrm{SRM}} = 1 - \frac{1}{16}\left(\sum_{m=1}^{4}\sqrt{\lambda_m}\right)^2, \tag{11}$$

where $\lambda_m = e^{-(g\alpha)^2}\sum_{n=1}^4 \exp[(1-m)\frac{2\pi i n}{4} + (g\alpha)^2 e^{\frac{2\pi i n}{4}}]$ are eigenvalues of the Gram matrix for QPSK signals. However, there remain major technical challenges in identifying physically realizable techniques to implement such strategies. In the following, we analyze the security of the four-state protocol under this SD attack.

III. SECURITY ANALYSIS OF FOUR-STATE PROTOCOL UNDER SD ATTACKS

Now we consider the security of the four-state CVQKD protocol under SD attacks; in particular, we consider the proposed intercept-resend attack strategy based on the SD receiver. In the four-state protocol, the channel features a transmission efficiency T and an excess noise ϵ, resulting in a noise variance of $(1 + T\epsilon)N_0$ at Bob's side, where N_0 is the shot-noise variance. Eve's attack strategy involves just optimizing her eavesdropping detection and applying the imperfection of a quantum channel to cover her eavesdropping. In a sense, there is always an eavesdropper if the quantum channel between Alice and Bob is imperfect, which corresponds to the environment. But it is fine, since Eve cannot learn anything about the final secret key obtained after privacy amplification if the security proof is correct.

The security of the four-state CVQKD scheme is investigated under general collective attacks in [20], since they are optimal in the asymptotic limit. The asymptotic secret key rate K is given by

$$K = \beta I_{\mathrm{AB}} - \chi_{\mathrm{BE}}, \tag{12}$$

where β is the reconciliation efficiency, I_{AB} is the classical mutual information between Alice and Bob, and χ_{BE} is the Holevo quantity

$$\chi_{\mathrm{BE}} = S(\rho_{\mathrm{E}}) - \sum_{m_{\mathrm{B}}} p(m_{\mathrm{B}}) S(\rho_{\mathrm{E}|m_{\mathrm{B}}}), \tag{13}$$

where $\rho_{\mathrm{E}} = \sum_{m_{\mathrm{B}}} p(m_{\mathrm{B}})\rho_{E|m_{\mathrm{B}}}$, m_{B} is the measurement of Bob, $p(m_{\mathrm{B}})$ is the probability density of the measurement, $\rho_{\mathrm{E}|m_{\mathrm{B}}}$ is Eve's state conditional on Bob's measurement result, and S is the Neumann entropy. According to the Gaussian optimality theorem [8], the Holevo information χ_{BE} between Eve and Bob is maximized when the state $\rho_{\mathrm{AB}} = |\Psi\rangle\langle\Psi|$ shared by Alice and Bob is Gaussian. Therefore, the quantity χ_{BE} can be upper bounded by a function of the covariance matrix Γ of the state ρ_{AB}, which is given by

$$\Gamma = \begin{pmatrix} V_{\mathrm{A}}\mathbb{I}_2 & \sqrt{T}Z\sigma_z \\ \sqrt{T}Z\sigma_z & (TV_{\mathrm{A}} + 1 + T\epsilon)\mathbb{I}_2 \end{pmatrix}, \tag{14}$$

where V_A is the variance of Alice's modulation in the P&M scheme, and Z is the correlation for the state $|\Psi\rangle$ in the form

$$Z = 2\alpha^2 \sum_{k=0}^{3} \frac{\lambda_{k-1}^{3/2}}{\lambda_k^{1/2}}. \qquad (15)$$

Actually, the covariance matrix Γ has the same form as in the Gaussian modulation scheme where Z is replaced by the correlation of a two-mode squeezed vacuum state $Z_{\mathrm{G}} = \sqrt{V_{\mathrm{A}}^2 + 2V_{\mathrm{A}}}$. When the modulation variance is sufficient low, Z will be almost equal to Z_{G}, and thus the bound on the maximum information available to Eve, χ_{BE}, is identical to the one obtained for a Gaussian modulation [20]. Using the fact that Eve's system purifies the system of Alice and Bob and $S(\rho_{\mathrm{E}|m_{\mathrm{B}}})$ is independent of m_{B} for a Gaussian scheme, the expression of χ_{BE} can be further simplified as

$$\chi_{\mathrm{BE}} = \sum_{i=1}^{2} G\left(\frac{\kappa_i - 1}{2}\right) - G\left(\frac{\kappa_3 - 1}{2}\right), \qquad (16)$$

where $G(x) = (x+1)\log_2(x+1) - x\log_2 x$, $\kappa_{1,2}$ are the symplectic eigenvalues of covariance matrix Γ, and κ_3 is the symplectic eigenvalue of the covariance matrix of the state $\rho_{\mathrm{A}|m_{\mathrm{B}}}$, which are given by

$$\kappa_{1,2} = \sqrt{\frac{1}{2}\left(A \pm \sqrt{A^2 - 4B}\right)}, \qquad (17)$$

$$\kappa_3 = \sqrt{\frac{\sqrt{B}(V_{\mathrm{A}}+1)}{TV_{\mathrm{A}} + 1 + T\epsilon}}, \qquad (18)$$

where

$$\begin{aligned} A &= (V_{\mathrm{A}}+1)^2 + (TV_{\mathrm{A}} + 1 + T\epsilon)^2 - 2TZ^2, \\ B &= [(V_{\mathrm{A}}+1)(TV_{\mathrm{A}} + 1 + T\epsilon) - TZ^2]^2. \end{aligned} \qquad (19)$$

Also, for the case of low modulation variance, the mutual information between Alice and Bob, I_{AB}, for homodyne detection can be evaluated as

$$I_{\mathrm{AB}} = \frac{1}{2}\log_2 \frac{TV_{\mathrm{A}} + 1 + T\epsilon}{1 + T\epsilon}. \qquad (20)$$

According to the shared absolute values and bits, they can evaluate the secret key rate for a general collective attack with linear channel assumption, and then estimate whether the communication is secure. It should be mentioned that in the four-state protocol, for both the P&M scheme and the EB scheme, Alice does not take a homodyne or heterodyne detection as in the Gaussian-modulated CVQKD protocol to obtain the values of quadratures X and P, but only knows the encoded bits. So Alice and Bob cannot evaluate the parameters T, ϵ of the quantum channel from the shared binary bits without linear channel assumption [37]. When Eve performs a concrete attack strategy, the sufficient condition for successful implementation is that the secret key rate estimated by the legitimated parties from their shard data is too large compared to its true value. If this is the case, they will extract a secret key which is too long, and therefore the scheme is not secure under the attack.

When Bob performs homodyne detection, the signs of Bob's measurement results $x_{\mathrm{B}}(p_{\mathrm{B}})$ correspond to the bits of the secret key, where the absolute values are independent of the secret key. It is because the bits of the secret key are not encoded on this variable but on the phase of the signal states. Thus, there may exist the case that Eve takes a fail discrimination and reproduces an error coherent state but with the correct sign of the quadrature x_{B} or p_{B}, and Eve will not introduce error bits in this case. While for the case of heterodyne detection, all of Eve's fail discriminations will incur error bits in the shared distributed binary string. For simplicity, we consider the case in which Bob performs homodyne detection and reverse reconciliation, and we suppose Eve's fail discriminations will all introduce error bits in the following.

We first evaluate the values of the transmission efficiency T_{e} and the excess noise ϵ_{e} of the quantum channel after Eve's SD attack. In order to capture the secret key without revealing herself, Eve will optimize the SD receiver, including improving the probability to successfully discriminate the coherent states $P_{\mathrm{c}} = 1 - P_{\mathrm{e}}$ and the efficiency of the SD receiver. Here we suppose Eve's SD receiver has perfect efficiency. Considering the probability of NLA, the state sent to Bob is changed to

$$\rho_{\mathrm{B}} = P_{\mathrm{s}}P_{\mathrm{c}}|\alpha_k\rangle\langle\alpha_k| + P_{\mathrm{s}}P_{\mathrm{e}}|\alpha_k'\rangle\langle\alpha_k'| + (1 - P_{\mathrm{s}})|0\rangle\langle 0|. \quad (21)$$

To hide herself, Eve will use a perfect quantum channel to substitute the noisy and lossy channel. Thus Bob will receive the identical state as ρ_{B}. It can be easily deduced that the transmission efficiency of the quantum channel is changed to

$$T_{\mathrm{e}} = P_{\mathrm{s}}P_{\mathrm{c}}. \qquad (22)$$

Also, we can see that the excess noise of the quantum channel comes from the vacuum state $|0\rangle$, the error state $|\alpha_k'\rangle$, and the shot noise; thus, the excess noise is given by

$$\epsilon_{\mathrm{e}} = \frac{V_{\mathrm{A}}P_{\mathrm{e}}}{1 - P_{\mathrm{e}}}. \qquad (23)$$

Meanwhile, the true mutual information between Bob and Eve, I_{BE}, can be seen as the classical information sent by Eve through the perfect quantum channel. When Bob is using homodyne detection, the mutual information I_{BE} can then be derived from Bob's measured variance $V_{\mathrm{B}} = P_{\mathrm{s}}V_{\mathrm{A}} + 1$ and the conditional variance $V_{\mathrm{B|E}} = P_{\mathrm{s}}P_{\mathrm{c}} + P_{\mathrm{s}}P_{\mathrm{e}} + 1 - P_{\mathrm{s}} = 1$ as

$$I_{\mathrm{BE}} = \tfrac{1}{2}\log_2(P_{\mathrm{s}}V_{\mathrm{A}} + 1). \qquad (24)$$

When the error probability of Eve's SD receiver reaches the SQL or Helstrom bound, the transmission efficiency and excess noise of the quantum channel after Eve's SD attack are then given by

$$T_{\mathrm{e}} = P_{\mathrm{s}}\left(1 - P_{\mathrm{SQL}}^{g}\right), \quad \epsilon_{\mathrm{e}} = \frac{V_{\mathrm{A}}P_{\mathrm{SQL}}^{g}}{1 - P_{\mathrm{SQL}}^{g}}, \qquad (25)$$

or

$$T_{\mathrm{e}} = P_{\mathrm{s}}\left(1 - P_{\mathrm{SRM}}^{g}\right), \quad \epsilon_{\mathrm{e}} = \frac{V_{\mathrm{A}}P_{\mathrm{SRM}}^{g}}{1 - P_{\mathrm{SRM}}^{g}}, \qquad (26)$$

respectively. So Alice and Bob can evaluate the Holevo information χ_{BE} and the mutual information I_{AB} between

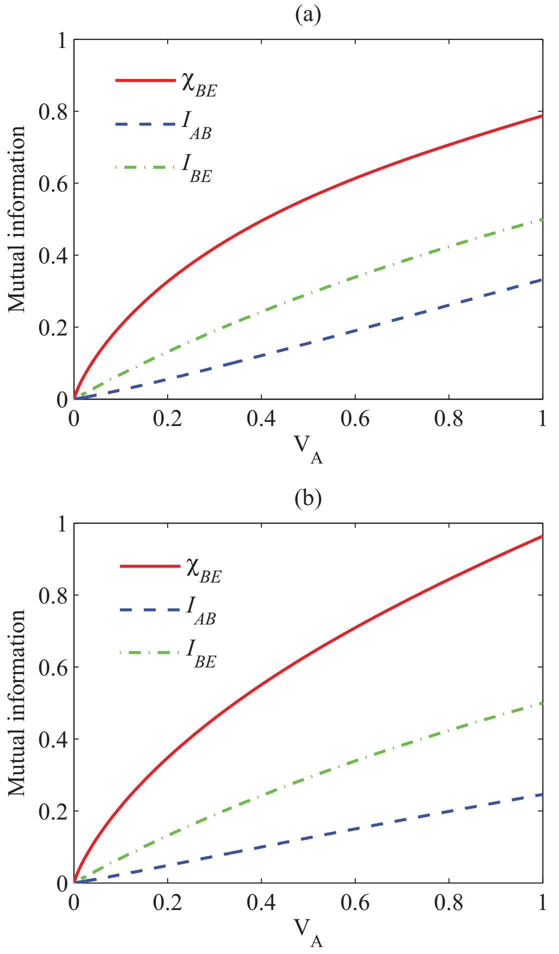

FIG. 2. (Color online) The mutual information $\chi_{\rm BE}$, $I_{\rm BE}$, and $I_{\rm AB}$ as a function of modulation variance $V_{\rm A}$ of the four-state protocol under the SD attack for $g = 1$, when the error probability of Eve's SD receiver $P_{\rm e}$ values are (a) $P^g_{\rm SRM}$ and (b) $P^g_{\rm SQL}$, respectively.

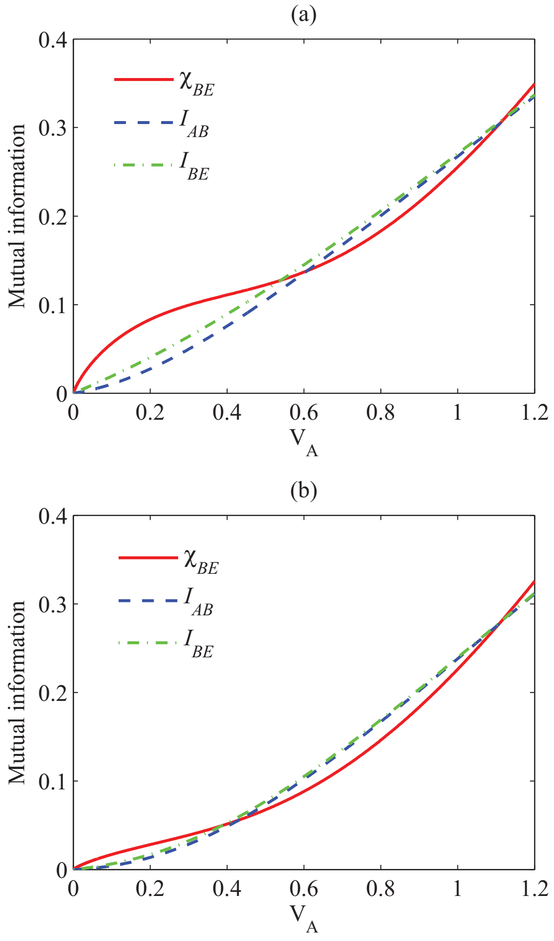

FIG. 3. (Color online) The mutual information $\chi_{\rm BE}$, $I_{\rm BE}$, and $I_{\rm AB}$ as a function of modulation variance $V_{\rm A}$ of the four-state protocol under the SD attack for (a) $g = 2$ when $P_{\rm e}$ values $P^g_{\rm SRM}$ and (b) $g = 4$ when $P_{\rm e}$ values $P^g_{\rm SQL}$, respectively.

Alice and Bob through Eqs. (16)–(20). In practice, the error probability of the discrimination receiver, $P_{\rm e}$, can be valued in the interval $[P^g_{\rm SRM}, P^g_{\rm SQL}]$. Supposing that Alice and Bob perform perfect reconciliation, the secret key rate inferred by Alice and Bob can be obtained as $K_{\rm infer} = I_{\rm AB} - \chi_{\rm BE}$.

Figure 2 shows the Holevo information $\chi_{\rm BE}$ inferred by Alice and Bob, the true mutual information $I_{\rm BE}$, and the mutual information $I_{\rm AB}$ between Alice and Bob as a function of modulation variance $V_{\rm A}$, where the NLA does not work, i.e., $g = 1$, and the error probability of Eve's SD receiver reaches the SQL or Helstrom bound, respectively. It can be seen from Fig. 2 that the Holevo information $\chi_{\rm BE}$ inferred by Alice and Bob is always larger than the true information $I_{\rm BE}$ revealed to Eve and the mutual information $I_{\rm AB}$ between Alice and Bob. Therefore, in this case Alice and Bob cannot extract a secure key and, also, Eve's attack is invalid.

When the NLA works, the mutual information values $\chi_{\rm BE}$, $I_{\rm BE}$, and $I_{\rm AB}$ are plotted in Fig. 3 as a function of modulation variance $V_{\rm A}$ for particular gain of the amplifier and SD receivers. Clearly, we can see that there always exists the case that the secret key rate $K_{\rm infer}$ inferred by Alice and Bob is positive but $\chi_{\rm BE} \leqslant I_{\rm BE}$ for proper modulation variance $V_{\rm A}$. Exactly, when the error probability of Eve's SD receiver reaches the Helstrom bound and setting $g = 2$, Alice and Bob will extract a string of the secret key after privacy amplification for the modulation variance $0.608 \leqslant V_{\rm A} \leqslant 1.109$ and they deem it secure. However, all this secret information has been obtained by Eve through the SD attack since $I_{\rm BE}$ is never less than $I_{\rm AB}$. Also, when the error probability of Eve's discrimination receiver reaches the SQL bound and setting $g = 4$, Eve can implement the SD attack successfully for the modulation variance $0.432 \leqslant V_{\rm A} \leqslant 1.107$.

Moreover, when increasing the gain of the amplifier, Eve can successfully implement the SD attack on the four-state protocol with much lower modulation variance. As shown in Fig. 4, when the error probability of Eve's discrimination receiver reaches the Helstrom or SQL bound and correspondingly setting $g = 4$ or $g = 6$, Eve can implement the SD attack successfully for the modulation variances $0.133 \leqslant V_{\rm A} \leqslant 1.135$ and $0.175 \leqslant V_{\rm A} \leqslant 1.135$, respectively. As proposed in [20,21], the optimal modulation variance for the four-state protocol is $V_{\rm A} = 0.3$, and the minimum gain of the amplifier should be $g^*_{\rm SRM} = 2.697$ and $g^*_{\rm SQL} = 4.663$ when Eve's discrimination receiver reaches Helstrom and SQL bounds, respectively. Physically, the use of NLA quite

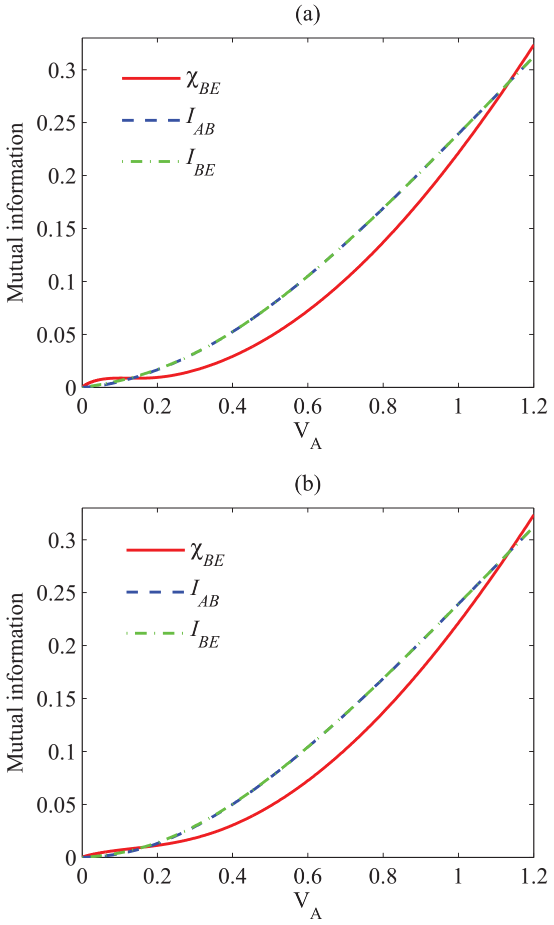

FIG. 4. (Color online) The mutual information χ_{BE}, I_{BE}, and I_{AB} as a function of modulation variance V_{A} of the four-state protocol under the SD attack for (a) $g = 4$ when P_{e} values P^{g}_{SRM} and (b) $g = 6$ when P_{e} values P^{g}_{SQL}, respectively.

decreases the error probability of the discrimination receiver and thus decreases the introduced excess noise, which makes the SD attack effective. It should be mentioned that the SD attack changes the transmission efficiency and the excess noise of the quantum channel. However, a sufficient condition for a successful attack is that the secret key rate estimated by the legitimate parties is larger than its true value. As analyzed above, when using an appropriate discrimination receiver and NLA, the mutual information between Eve and Bob calculated under the general collective attack, i.e., the Holevo information χ_{BE} inferred by Alice and Bob, will be smaller than its true value, while Alice and Bob can correctly evaluate the true value of the mutual information between them, i.e., I_{AB}. Thus, the secret key rate K_{infer} inferred by Alice and Bob will be larger than its true value, whatever error correction method is applied. Moreover, the modification of the privacy amplification method here is also invalid to prevent the SD attack, since the Holevo information χ_{BE} inferred by Alice and Bob has limited the maximum key information that Alice and Bob will discard from the compression of their shared key information in the privacy amplification procedure. In summary, we can conclude that Eve can successfully implement the SD attack and the original four-state scheme is not secure.

IV. SECURITY OF THE FOUR-STATE PROTOCOL WITH DECOY STATES UNDER SD ATTACKS

Intuitionally, the main reason for weak security of the original four-state protocol is that the use of discretely modulated signal states makes Eve's eavesdropping possible by using a discrimination receiver. Also, Leverrier and Grangier clarify in [37] that a crucial step of the unconditional security proof of the original four-state protocol relies on the hidden assumption that the quantum channel is linear; that is, the input-output relations of the quadrature operators in the Heisenberg representation can be given by

$$\begin{aligned} X_{\mathrm{out}} &= g_{\mathrm{X}} X_{\mathrm{in}} + B_{\mathrm{X}}, \\ P_{\mathrm{out}} &= g_{\mathrm{P}} P_{\mathrm{in}} + B_{\mathrm{P}}, \end{aligned} \tag{27}$$

where $B_{\mathrm{X}}, B_{\mathrm{P}}$ are uncorrelated added noises with the input quadratures $X_{\mathrm{in}}, P_{\mathrm{in}}$. Actually, in the EB version of the original four-state protocol, Alice's measurement only discriminates which coherent state is sent to Bob and does not measure the quadratures of her mode. Thus, Alice and Bob cannot estimate the covariance matrix from their experimental data without the linear channel assumption.

To solve this problem, an improved four-state protocol with decoy states [21] is proposed such that the mixed state sent to Bob is Gaussian as

$$p\sigma_{\mathrm{key}} + (1 - p)\sigma_{\mathrm{decoy}} = \sigma_{\mathrm{G}}, \tag{28}$$

where σ_{key} is the state used for the key distillation and σ_{decoy} is the decoy state. Alice randomly prepares σ_{key} and σ_{decoy} with probability p and $1 - p$, respectively, such that the mixed state sent to Bob is Gaussian state σ_{G}. So Alice can randomly use the Gaussian state σ_{G} to perform parameter estimation or use σ_{key} for key distribution. If a state is used for parameter estimation, in the EB scheme, Alice simply performs a heterodyne detection on her part and Bob proceeds as usual. At the end of the protocol, Alice and Bob can exchange their statistics and construct the covariance matrix of the two-mode Gaussian state after the quantum channel, which removes the hypothesis of the linear quantum channel.

When Alice and Bob introduce decoy states, Eve cannot distinguish whether the state is σ_{key}, σ_{decoy}, or σ_{G}. Thus, Eve's intercept-resend attack will inevitably introduce too much excess noise and incur a negative secret key rate, since the discrimination receiver is noneffective for Gaussian states, whereas in Gaussian-modulated CVQKD schemes, the key information is encoded in both the amplitudes and the phases of the signal states, which are not QPSK signals anymore. So in this case, the SD attacks will be not more effective than the general collective attacks analyzed in [21]. Therefore, Alice can safely choose non-Gaussian modulation to distribute the secret key, since the introduction of decoy states makes the protocol secure against arbitrary collective attacks and also against the intercept-resend attack based on the discrimination receiver. However, accurate preparation of a decoy state is a thorny issue in practice, which may increase the difficulty of experimental implementation of the discretely modulated protocols.

Actually, Eve's SD attack makes the quantum channel between Alice and Bob nonlinear, since Eve's NLA is nondeterministic and the discrimination receiver is probabilistic, and one can never obtain such input-output relations as in Eq. (16) after Eve's SD attack. Thus, the security proof in the original four-state protocol against a general collective attack excludes the proposed SD attack, which may result in a better performance in eavesdropping secret information from Bob's side. Therefore, it can be concluded that the assumption of a linear quantum channel produces a loophole for the intercept-resend attack based on the discrimination receiver, and there may exist other types of feasible nonlinear attacks, since the security has been proved under the linear attacks in [20]. Moreover, we can conclude that the decoy states are indispensable for secure communication via discretely modulated CVQKD, and minor or straightforward modifications of the original protocols, such as the modifications of the error correction and privacy amplification, cannot prevent the SD attack, because these modifications cannot fundamentally rectify the incorrect bound on the key information leaked to Eve by the legitimate parties.

V. CONCLUSION

We have investigated the security of the discretely modulated CVQKD protocol under SD attacks and, in particular, we considered the security of the original four-state protocol and the one with decoy states under Eve's SD attacks. For simplicity, we consider the security under the intercept-resend attack strategy based on a SD receiver and a heralded NLA for homodyne detection and reverse reconciliation. The results of the security analysis reveal that the secret key rate inferred by Alice and Bob is larger than its true value under the proposed intercept-resend attack. However, it should be mentioned that it does not mean the proposed SD attack is optimal. Therefore, Eve can obtain the secret information without being revealed by Alice and Bob, and the original four-state protocol is not secure. Moreover, we show the decoy states can be well applied to resist the proposed SD attack. Actually, the four-state protocol itself provides the loophole for the intercept-resend attack based on a discrimination receiver, since its security proof is obtained on the assumption that the quantum channel is linear. However, the difficulty of accurate preparation of decoy states makes the implementation of discretely modulated protocols complicated.

ACKNOWLEDGMENTS

We are grateful to an anonymous referee for his fruitful suggestions. This work was supported by the National Natural Science Foundation of China (Grants No. 61170228 and No. 61332019), the China Postdoctoral Science Foundation (Grant No. 2013M540365), and the Shanghai Jiao Tong University Postdoctoral Research Foundation (Grant No. AE606203).

[1] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, Rev. Mod. Phys. **81**, 1301 (2009).

[2] F. Grosshans and P. Grangier, Phys. Rev. Lett. **88**, 057902 (2002).

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

[4] C. Weedbrook, A. M. Lance, W. P. Bowen, T. Symul, T. C. Ralph, and P. K. Lam, Phys. Rev. Lett. **93**, 170504 (2004).

[5] A. M. Lance, T. Symul, V. Sharma, C. Weedbrook, T. C. Ralph, and P. K. Lam, Phys. Rev. Lett. **95**, 180503 (2005).

[6] J. Lodewyck, M. Bloch, R. García-Patrón, S. Fossier, E. Karpov, E. Diamanti, T. Debuisschert, N. J. Cerf, R. Tualle-Brouri, S. W. McLaughlin, and P. Grangier, Phys. Rev. A **76**, 042305 (2007).

[7] C. Weedbrook, S. Pirandola, R. García-Patrón, N. J. Cerf, T. C. Ralph, J. H. Shapiro, and S. Lloyd, Rev. Mod. Phys. **84**, 621 (2012).

[8] R. García-Patrón and N. J. Cerf, Phys. Rev. Lett. **97**, 190503 (2006).

[9] M. Navascués, F. Grosshans, and A. Acín, Phys. Rev. Lett. **97**, 190502 (2006).

[10] A. Leverrier, F. Grosshans, and P. Grangier, Phys. Rev. A **81**, 062343 (2010).

[11] R. Renner and J. I. Cirac, Phys. Rev. Lett. **102**, 110504 (2009).

[12] A. Leverrier, R. García-Patrón, R. Renner, and N. J. Cerf, Phys. Rev. Lett. **110**, 030502 (2013).

[13] F. Furrer, T. Franz, M. Berta, A. Leverrier, V. B. Scholz, M. Tomamichel, and R. F. Werner, Phys. Rev. Lett. **109**, 100502 (2012).

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

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

[16] A. Leverrier, R. Alléaume, J. Boutros, G. Zémor, and P. Grangier, Phys. Rev. A **77**, 042325 (2008).

[17] P. Jouguet, S. Kunz-Jacques, and A. Leverrier, Phys. Rev. A **84**, 062317 (2011).

[18] R. Blandino, A. Leverrier, M. Barbieri, J. Etesse, P. Grangier, and R. Tualle-Brouri, Phys. Rev. A **86**, 012327 (2012).

[19] P. Huang, G. He, J. Fang, and G. Zeng, Phys. Rev. A **87**, 012317 (2013).

[20] A. Leverrier and P. Grangier, Phys. Rev. Lett. **102**, 180504 (2009).

[21] A. Leverrier and P. Grangier, Phys. Rev. A **83**, 042312 (2011).

[22] K. Tsujino, D. Fukuda, G. Fujii, S. Inoue, M. Fujiwara, M. Takeoka, and M. Sasaki, Phys. Rev. Lett. **106**, 250503 (2011).

[23] F. E. Becerra, J. Fan, G. Baumgartner, S. V. Polyakov, J. Goldhar, J. T. Kosloski, and A. Migdall, Phys. Rev. A **84**, 062324 (2011).

[24] F. E. Becerra, J. Fan, G. Baumgartner, J. Goldhar, J. T. Kosloski, and A. Migdall, Nat. Photonics **7**, 147 (2013).

[25] T. C. Ralph and A. P. Lund, in *Quantum Communication Measurement and Computing (QCMC): The 9th International Conference, Calgary, Canada, 19–24 August 2008*, edited by A. Lvovsky, AIP Conf. Proc. No. 1110 (AIP, New York, 2009), pp. 155–160.

[26] F. Ferreyrol, M. Barbieri, R. Blandino, S. Fossier, R. Tualle-Brouri, and P. Grangier, Phys. Rev. Lett. **104**, 123603 (2010).

[27] F. Ferreyrol, R. Blandino, M. Barbieri, R. Tualle-Brouri, and P. Grangier, Phys. Rev. A **83**, 063801 (2011).

[28] M. Barbieri, F. Ferreyrol, R. Blandino, R. Tualle-Brouri, and P. Grangier, Laser Phys. Lett. **8**, 411 (2011).

[29] A. Zavatta, J. Fiurasek, and M. Bellini, Nat. Photonics **5**, 52 (2011).

[30] G. Y. Xiang, T. C. Ralph, A. P. Lund, N. Walk, and G. J. Pryde, Nat. Photonics **4**, 316 (2010).

[31] M. A. Usuga, C. R. Muller, C. Wittmann, P. Marek, R. Filip, C. Marquardt, G. Leuchs, and U. L. Andersen, Nat. Phys. **6**, 767 (2010).

[32] Y. B. Zhao, M. Heid, J. Rigas, and N. Lutkenhaus, Phys. Rev. A **79**, 012307 (2009).

[33] D. Sych and G. Leuchs, New J. Phys. **12**, 053019 (2010).

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

[35] C. W. Helstrom, *Quantum Detection and Estimation Theory, Mathematics in Science and Engineering* (Academic, New York, 1976), Vol. 123.

[36] K. Kato, M. Osaki, M. Sasaki, and O. Hirota, IEEE Trans. Commun. **47**, 248 (1999).

[37] A. Leverrier and P. Grangier, Phys. Rev. Lett. **106**, 259902(E) (2011).