Int J Theor Phys (2013) 52:4174–4184
DOI 10.1007/s10773-013-1730-0

Continuous Variable Quantum Secret Sharing via Quantum Teleportation

Nan-run Zhou · Han-chong Song · Li-hua Gong

Received: 28 April 2013 / Accepted: 2 July 2013 / Published online: 26 July 2013

Abstract A continuous variable quantum secret sharing (CVQSS) scheme is proposed by using quantum teleportation. In the scheme, the participants Bob and Charlie can recover the classical secret keys only when they cooperate. Meanwhile, the security of the CVQSS scheme is analyzed in detail by calculating the bit error rates (BERs) under different situations. It is shown that our proposed CVQSS scheme not only can resist the external attacks, but also can against the participant's malicious attacks when the channel transmission efficiency η is above 50 %.

Keywords Continuous variable · Quantum secret sharing · Quantum teleportation · Bit error rate

1 Introduction

Secret sharing is one of the important research directions in cryptography. It allows a sender to split her message into n parts between n participants respectively; neither $n-1$ nor fewer participants can read out the message only if all the n participants cooperate. Classical secret sharing schemes mainly are designed based on some complex algorithms or unsolved problems, however they can not overcome the problem of Catch22 [1]. Quantum secret sharing (QSS) schemes mainly depend on the quantum no-cloning theorem and the Heisenberg uncertainty principle, which ensure the unconditional security of perfectly designed QSS schemes. Therefore, QSS has attracted lots of attentions and developed rapidly since it was first presented.

N. Zhou (✉) · H. Song · L. Gong
Department of Electronic Information Engineering, Nanchang University, Nanchang 330031, China
e-mail: znr21@163.com

N. Zhou · L. Gong
Information Security Center, Beijing University of Posts and Telecommunications, Beijing 100876, China

In 1999, Hillery M. et al. proposed the first QSS scheme based on GHZ states, where the two parts can recover the secret key when they choose the same measurement basis [2]. Utilizing the quantum error correcting codes, Cleve R. et al. gave an efficient construction of a (k, n) threshold scheme [3]. From then on, a variety of QSS schemes have been put forward in both theoretical [4–16] and experimental [17, 18] aspects. According to the different properties of the carriers used, the QSS protocols can be generally classified into two types, i.e., discrete variable quantum secret sharing (DVQSS) schemes [2–16] and continuous variable quantum secret sharing (CVQSS) schemes [19–22]. DVQSS schemes mainly use the single photons or weak laser pulses as their information carriers. DVQSS schemes are difficult to satisfy the communication demands nowadays due to the low channel capacity and the difficulty of the preparation of single photons. Fortunately, CVQSS schemes utilize the continuous variable quantum states to share the secrets, where the states, such as coherent states, squeezed states can be easily generated and operated by linear optical components. Furthermore, these states can greatly improve the channel capacity, thus the CVQSS schemes are expected to play a key role in future integrated continuous variable quantum information systems. Tyc T. et al. developed a continuous-variable quantum secret sharing framework with its interferometric realization, which needs infinite squeezing [19]. Lance A.M. et al. performed two experimental (2, 3) threshold QSS schemes using entangled beams [20]. Later, encoding a secret coherent state into a tripartite entangled state and distributing to three players, Lance A.M. et al. achieved a fidelity average over all reconstruction permutations of 0.73 ± 0.02 in experiment [21]. Xie C.D. et al. proposed a quantum state sharing scheme with continuous variables, in which the single-mode squeezed states are applied to enhance the security of information in quantum teleportation network [22].

These protocols in Refs. [19–22], however, share not the classical secret itself but quantum state. The secret shares obtained by the agents only allow them to build an unknown quantum state. These protocols are not applicable to share a classical secret directly. Here, we present a CVQSS scheme utilizing the squeezed state to carry the secret and the quantum teleportation to deliver the secret. Unlike protocols in Refs. [19–22] sharing quantum states finally, our scheme directly shares classic bits and does not need infinite squeezing.

The rest of this paper is organized as follows. In Sect. 2, some basic knowledge is related in order to introduce the proposed scheme in a compact way in Sect. 3. In Sect. 4, the security of the proposed scheme is analyzed in detail by calculating the bit error rates under different situations. The conclusion is drawn in Sect. 5.

2 Basic Knowledge

2.1 Two-Mode Squeezed Vacuum State

In quantum optics, the squeezed vacuum state is:

$$a = x + \mathrm{i}p = e^{r}x(0) + \mathrm{i}e^{-r}p(0), \tag{1}$$

where $x(0)$, $p(0)$ are the amplitude and the phase of the initial vacuum state and they follows a Gaussian probability distribution $x(0)$, $p(0) \sim N(0, 1)$, $[x(0), p(0)] = 2\mathrm{i}$, r is the squeezed parameter, the amplitude is squeezed when $r < 0$ while the phase is squeezed when $r > 0$. There is a relation between the amplitude and the phase under the Heisenberg uncertainty principle: $\Delta x \cdot \Delta p \geq 1$.

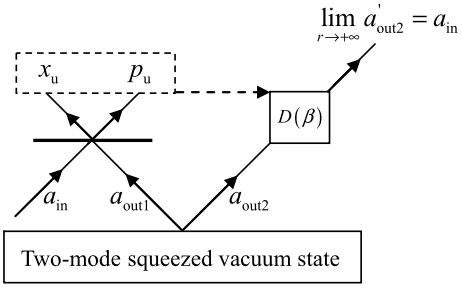


Fig. 1 Schematic of quantum teleportation

Similarly, the two-mode squeezed vacuum state can be generated by combining an amplitude-squeezed vacuum state with a phase-squeezed vacuum state by a half beam splitter, then the amplitudes and the phases of the two output modes are [23]:

$$x_{\text{out1}} = \frac{1}{\sqrt{2}} e^{r} x_{\text{in1}}(0) + \frac{1}{\sqrt{2}} e^{-r} x_{\text{in2}}(0), \tag{2a}$$

$$p_{\text{out1}} = \frac{1}{\sqrt{2}} e^{-r} p_{\text{in1}}(0) + \frac{1}{\sqrt{2}} e^{r} p_{\text{in2}}(0), \tag{2b}$$

$$x_{\text{out2}} = \frac{1}{\sqrt{2}} e^{r} x_{\text{in1}}(0) - \frac{1}{\sqrt{2}} e^{-r} x_{\text{in2}}(0), \tag{2c}$$

$$p_{\text{out2}} = \frac{1}{\sqrt{2}} e^{-r} p_{\text{in1}}(0) - \frac{1}{\sqrt{2}} e^{r} p_{\text{in2}}(0). \tag{2d}$$

The two output modes have the following correlations:

$$\left\langle \left[\Delta(x_{\text{out1}} \mp x_{\text{out2}}) \right]^2 \right\rangle = \left\langle \left[\Delta(p_{\text{out1}} \pm p_{\text{out2}}) \right]^2 \right\rangle = 2e^{\mp 2r}. \tag{3}$$

From Eq. (3), one can see that the correlation between a_{out1} and a_{out2} becomes perfect as the squeezed parameter r increases:

$$\lim_{r\to+\infty} x_{\text{out1}} = x_{\text{out2}}, \qquad \lim_{r\to+\infty} p_{\text{out1}} = -p_{\text{out2}}, \tag{4}$$

2.2 Continuous Variable Quantum Teleportation

Quantum teleportation is an important ingredient in quantum information science, which enables reliable transfer of an arbitrary, unknown quantum state from one location to another. Figure 1 is the schematic of quantum teleportation. Suppose two distant players Alice and Bob share the two-mode squeezed vacuum state a_{out1}, a_{out2}, when Alice performs a Bell measurement on a_{out1} and an unknown input $a_{\text{in}} = x_{\text{in}} + \text{i}p_{\text{in}}$, she can obtain:

$$x_{\text{u}} = \frac{1}{\sqrt{2}}(x_{\text{in}} - x_{\text{out1}}), \qquad p_{\text{u}} = \frac{1}{\sqrt{2}}(p_{\text{in}} + p_{\text{out1}}). \tag{5}$$

Then Bob's mode a_{out2} can be rewritten as [24]:

$$x_{\text{out2}} = x_{\text{out2}} + \sqrt{2}x_{\text{u}} - \sqrt{2}x_{\text{u}} = x_{\text{in}} - (x_{\text{out1}} - x_{\text{out2}}) - \sqrt{2}x_{\text{u}}, \tag{6}$$

$$p_{\text{out2}} = p_{\text{out2}} + \sqrt{2}p_{\text{u}} - \sqrt{2}p_{\text{u}} = p_{\text{in}} + (p_{\text{out1}} + p_{\text{out2}}) - \sqrt{2}p_{\text{u}}. \tag{7}$$

Note that a_{out2} does not differ much from the original unknown input a_{in} beside a displacement operator. From Eqs. (4) and (6), (7), the original input a_{in} can be easily reconstructed by a unitary operation $D(\beta = \sqrt{2}x_{\text{u}} + \text{i}\sqrt{2}p_{\text{u}})$ on a_{out2} when the entanglement degree is high enough.

2.3 Binary Bit Modulation

For an arbitrary quantum state $\varphi = x_\phi + \mathrm{i}p_\phi$, where x_ϕ, $p_\phi \sim N(\mu, \sigma^2)$, how is the secret key modulated on the amplitude? If one wants to send bit 1, then he puts a positive modulation A on the amplitude, where A is a positive constant. While if one wants to send bit 0, then he does nothing. In the ideal condition ($\sigma^2 = 0$), when demodulating the signal, one can obtain only two results μ and $\mu + A$, corresponding to 0 and 1 respectively. However, the variance σ^2 of the signal's amplitude is always positive, this means that the results obtained are not the exact two constants μ and $\mu + A$ all the time but with fluctuations. Denote bit 0 by the result $x_\phi < \mu + \frac{A}{2}$ while bit 1 by $x_\phi \geq \mu + \frac{A}{2}$. Also, one should pay attention to two situations which will cause errors, one is that the measurement result $x_\phi \geq \mu + \frac{A}{2}$ when sending bit 0, i.e., bit 0 is turned into bit 1, the other is that the measurement result $x_\phi < \mu + \frac{A}{2}$ when sending bit 1, i.e., bit 1 is turned into bit 0. The bit error rate is an important security evaluation in QSS scheme, if the bit error rate is higher than the specific error threshold, then the channel is not secure. Likewise, the binary bit modulation is also appropriate for the signal's phase quadrature.

3 Continuous Variable Quantum Secret Sharing Scheme

3.1 Principles

Continuous variable quantum teleportation can be used to realize CVQSS. If Alice wants to share a secret key with Bob and Charlie, she only needs Bob to send a squeezed state to her, and then she modulates the squeezed state according to her secret bits and transfers the resulting state to Charlie via quantum teleportation. At this point, Charlie owns the quantum state carrying the bits. However, Charlie does not know which component is squeezed. Particularly, Charlie can get no secret key alone even if he chooses the right measurement basis if Bob adds some initial information on the squeezed state. Accordingly, although Bob knows which component is squeezed, he can also get little useful information since he does not own the quantum state as Charlie. As a result, the secret key can only be recovered when Bob and Charlie cooperate.

3.2 Continuous Variable Quantum Secret Sharing Scheme

Suppose Alice wants to share a classical secret key with two distant agents Bob and Charlie. Then the two receivers, Bob and Charlie, can infer the secret message only by their mutual assistances. The CVQSS scheme shown in Fig. 2 involves the following steps:

(1) Bob applies a squeezed operator $S(r_1)$ on the vacuum state $|0\rangle_1$ to generate the squeezed vacuum state a_1, while $S(r_1)$ depends on Bob's pre-prepared random bit string n_B with $p(n_B = 0) = p(n_B = 1) = \frac{1}{2}$. If $n_B = 0$, Bob uses $r_1 < 0$, i.e., a_1 is an amplitude squeezed state, then Bob puts a modulation on a_1 with a displacement operator $D(\alpha_1 = A)$. If $n_B = 1$, Bob uses $r_1 > 0$, i.e., a_1 is a phase squeezed state, then Bob puts a modulation on a_1 with a displacement operator $D(\alpha_1 = \mathrm{i}A)$. Lastly, Bob randomly selects some time slots t_1 to insert the coherent states $a_1' = |x_1' + \mathrm{i}p_1'\rangle$ into a_1 and sends it to Alice together.

(2) On receiving the state a_2, Alice returns an acknowledgement to Bob. The state a_2 is the same as a_1 when Eve is absent in the quantum channel.

(3) Bob publishes the corresponding time slots t_1, along with the amplitude x_1' and the phase p_1' of the coherent state a_1'.

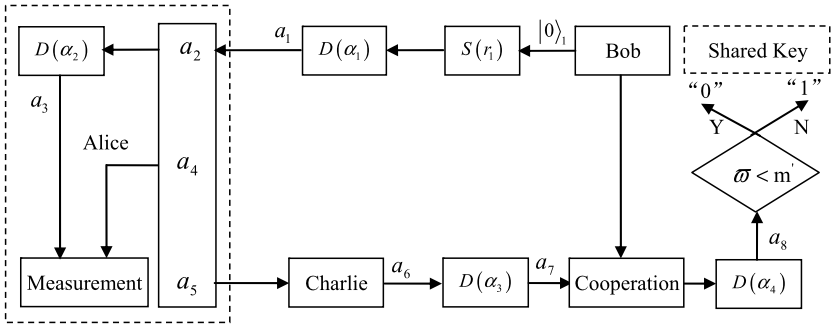


Fig. 2 Schematic of the CVQSS scheme

(4) After hearing from Bob, Alice takes a random measurement on the amplitude or the phase of a_2, and then she compares her measurement results with Bob's corresponding data to detect eavesdropping. If the error rate does not exceed certain threshold, Alice and Bob confirms the quantum channel is secure, then Alice removes the coherent states in a_2 and goes to next step; or else, Alice terminates communication.

(5) Alice applies a unitary operation $D(\alpha_2 = x + \mathrm{i}x)$ on a_2 to generate a_3 according to the secret key. In this scheme, we formulate Alice uses the binary bit modulation and the secret bits 0 and 1 correspond to $x = B$ and $x = B + V_s$, respectively, where the B and V_s are two constants. Apparently, the amplitude x_3 and the phase p_3 of a_3 are still Gaussian variables. Without loss of generality, we suppose x_3, $p_3 \sim N(\mu, \sigma^2)$ and the measurement results $\varpi \geq \mu + B + \frac{V_s}{2}$, $\varpi < \mu + B + \frac{V_s}{2}$ stand for bits 1 and 0, respectively.

(6) Alice prepares the two mode squeezed vacuum states a_4, a_5 and transmits a_5 to Charlie.

(7) Charlie declares he has received the state a_6, and then he measures either the amplitude or the phase of a_6 in some random time slots t_2. After the measurement, Charlie publishes the time slots t_2, the measurement component and the measurement results. a_6 is the same as a_5 if Eve is absent in the quantum channel.

(8) Alice chooses the same measurement component as Charlie at t_2 to detect eavesdropping. On the basis of the entanglement properties of two-mode squeezed state, there exist correlations between a_4 and a_6, i.e., $(x_4 - x_6)^2 \to 0$ and $(p_4 + p_6)^2 \to 0$. If the measurement result does not exceed certain error threshold, Alice goes to next step; otherwise, she returns to step 6.

(9) Alice does a joint Bell measurement on a_3 and a_4 with the outcomes $x_{\mathrm{u}} = \frac{1}{\sqrt{2}}(x_3 - x_4)$ and $p_{\mathrm{u}} = \frac{1}{\sqrt{2}}(p_3 + p_4)$, then she publishes x_{u}, p_{u} and the judgment threshold $m = B + \frac{V_s}{2}$.

(10) Charlie applies a unitary operation $D(\alpha_3 = \sqrt{2\eta_2}(x_{\mathrm{u}} + \mathrm{i}p_{\mathrm{u}}))$ on a_6 to get a_7.

(11) Bob and Charlie cooperate to recover the shared secret keys. As what is required in the QSS [2, 3], the recovery processes can only be done when Bob and Charlie come together. If $n_B = 0$, Bob and Charlie apply a unitary operation $D(\alpha_4 = -\sqrt{\eta_1\eta_2}e^{-r_1}A)$ on a_7 to get a_8, and then they measure the amplitude of a_8, where η_1, η_2 are the transmission efficiencies of the quantum channels from Bob to Alice and from Alice to Charlie, respectively. If $n_B = 1$, Bob and Charlie apply a unitary operation $D(\alpha_4 = -\mathrm{i}\sqrt{\eta_1\eta_2}e^{-r_1}\mathrm{A})$ on a_7, and then they measure the phase of a_8. Finally, Bob and Charlie recover the shared secret keys according to the judgment threshold $m' = \sqrt{\eta_2}m$. It denotes the secret key is 0 if the measurement result $\varpi < m'$, while the secret key is 1 if $\varpi \geq m'$.

In this CVQSS scheme, the steps (1)–(4) are the preparation and transmission processes of the squeezed state. To some extent, the squeezed states can be transmitted from Bob to Alice securely via quantum teleportation like steps (6)–(10). However, this will make the schemes complicated. For this reason, just the squeezed states are transmitted directly and the coherent states are inserted to detect the eavesdropping in the channel. Also, some displacements on the squeezed component of the squeezed state are added to protect the secret. The purpose of step (5) is to put classical bits on the quantum signal with binary bit modulation. Although the secret keys are modulated on both the amplitude and the phase of the squeezed states, they can only be demodulated on the squeezed component due to the large variance of the unsqueezed component. Notice that if Alice sends her states to Charlie directly like step (1), Bob can eavesdrop all of the states and select the right component to measure them, then Bob can obtain all the secrets. Thus, quantum teleportation is employed to avoid this attack. Steps (6)–(10) are the processes of quantum teleportation, Alice can teleport the squeezed state carrying the shared keys to Charlie without moving it if the two mode squeezed vacuum state has a high degree of entanglement. Finally, if Bob and Charlie cooperate, they can recover the shared keys with step (11), all the squeezed states they owned can be measured on the right components with the help of Bob's information, that is to say, every squeezed states can be used to rebuild the keys.

4 Security Analyses

Compared with quantum key distribution protocols, the QSS schemes have a higher demand on the security since one should consider not only the external eavesdropper Eve's attacks, but also the dishonest participant's malicious attacks. Moreover, the dishonest participant is more likely to get the secret keys, since they possess more resource than Eve. Thus the security of the secret against the dishonest participants is the primary goal in the QSS scheme. If a scheme is secure to the dishonest participants, it can naturally against the external attacks [25]. In our scheme, Eve has no information about Bob's squeezed state, and she does not know which component of the quantum state is squeezed. She does not possess the quantum state carrying the secret keys either. Therefore, the participants Bob and Charlie have more advantages than Eve in our scheme and the CVQSS scheme is secure if it can resist Bob or Charlie's attacks.

4.1 BER Without Eavesdropping

In the CVQSS scheme, Bob prepares the initial squeezed state a_1 according to his pre-prepared random bit string n_B. If $n_B = 0$, a_1 can be expressed as:

$$x_1 = e^{-r_1}\big(x_1(0) + A\big), \qquad p_1 = e^{r_1} p_1(0), \tag{8}$$

where $r_1 > 0$, or else:

$$x_1 = e^{r_1} x_1(0), \qquad p_1 = e^{-r_1}\big(p_1(0) + A\big). \tag{9}$$

Then Alice's state a_2 is:

$$x_2 = \sqrt{\eta_1} x_1 + \sqrt{1-\eta_1} x_{\mathrm{N1}}, \qquad p_2 = \sqrt{\eta_1} p_1 + \sqrt{1-\eta_1} p_{\mathrm{N1}}, \tag{10}$$

where x_{N1}, p_{N1} represent the noise in the quantum channel from Bob to Alice, x_{N1}, $p_{\mathrm{N1}} \sim N(0, 1)$. After the unitary operation $D(\alpha_2 = x + \mathrm{i}x)$, Alice obtains a_3:

$$x_3 = x_2 + x, \qquad p_3 = p_2 + x. \tag{11}$$

According to Eqs. (2a)–(2d), the two-mode squeezed vacuum states a_4 and a_5 are given by:

$$x_4 = \frac{1}{\sqrt{2}}\left(e^{r_2}x_{\text{in1}}(0) + e^{-r_2}x_{\text{in2}}(0)\right), \tag{12a}$$

$$p_4 = \frac{1}{\sqrt{2}}\left(e^{-r_2}p_{\text{in1}}(0) + e^{r_2}p_{\text{in2}}(0)\right), \tag{12b}$$

$$x_5 = \frac{1}{\sqrt{2}}\left(e^{r_2}x_{\text{in1}}(0) - e^{-r_2}x_{\text{in2}}(0)\right), \tag{12c}$$

$$p_5 = \frac{1}{\sqrt{2}}\left(e^{-r_2}p_{\text{in1}}(0) - e^{r_2}p_{\text{in2}}(0)\right). \tag{12d}$$

Alice sends a_5 to Charlie, and then Charlie's state a_6 is:

$$x_6 = \sqrt{\eta_2}x_5 + \sqrt{1-\eta_2}x_{\text{N2}}, \qquad p_6 = \sqrt{\eta_2}p_5 + \sqrt{1-\eta_2}p_{\text{N2}}. \tag{13}$$

Similarly, x_{N2}, p_{N2} represent the noise in the quantum channel from Alice to Charlie, x_{N2}, $p_{\text{N2}} \sim N(0,1)$. If the quantum channel is secure, Alice makes a joint Bell measurement on a_3 and a_4:

$$x_{\text{u}} = \frac{1}{\sqrt{2}}(x_3 - x_4), \qquad p_{\text{u}} = \frac{1}{\sqrt{2}}(p_3 + p_4). \tag{14}$$

Since the amplitude and the phase in a quantum state are symmetric, the BER will be same despite of amplitude squeezed state or phase squeezed state. In the process of secret recovery, without loss of generality, the situation of amplitude squeezed state Bob prepared is analyzed. After quantum teleportation, the amplitude of Charlie's state a_7 is:

$$x_7 = x_6 + \sqrt{2\eta_2}x_{\text{u}}. \tag{15}$$

If there is no eavesdropping, Bob and Charlie cooperate to apply a unitary operation $D(\alpha_4 = -\sqrt{\eta_1\eta_2}e^{-r_1}A)$ on a_7 to rebuild the secret. If Alice wants to send bit 0, then $x = B$. By recalling Eq. (8) and Eqs. (10)–(15), x_8 turns out to be:

$$\begin{aligned} x_8 = {} & \sqrt{\eta_2}B + \sqrt{\eta_1\eta_2}e^{-r_1}x_1(0) + \sqrt{(1-\eta_1)\eta_2}x_{\text{N1}} + \sqrt{1-\eta_2}x_{\text{N2}} \\ & - \sqrt{2\eta_2}e^{-r_2}x_{\text{in2}}(0). \end{aligned} \tag{16}$$

Apparently, x_8 is a Gaussian variable, $x_8 \sim N(\sqrt{\eta_2}B, \sigma_8^2)$, $\sigma_8^2 = 1 + \eta_1\eta_2(e^{-2r_1} - 1) + 2\eta_2 e^{-2r_2}$. If $x_8 < \sqrt{\eta_2}(B + \frac{V_s}{2})$, then Bob and Charlie can demodulate and get the right bit 0; or else, they will get the wrong bit 1. Thus the BER of bit 0 can be calculated as:

$$p_{0\text{err}}(B,C) = \int_{\sqrt{\eta_2}(B+\frac{V_s}{2})}^{\infty} \frac{1}{\sqrt{2\pi\sigma_8^2}} e^{-\frac{(x-\sqrt{\eta_2}B)^2}{2\sigma_8^2}} \,\mathrm{d}x. \tag{17}$$

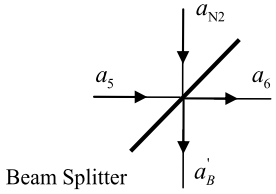
Similarly, the BER of bit 1 is:

$$p_{1\text{err}}(B,C) = \int_{-\infty}^{\sqrt{\eta_2}(B+\frac{V_s}{2})} \frac{1}{\sqrt{2\pi\sigma_8^2}} e^{-\frac{(x-\sqrt{\eta_2}(B+V_s))^2}{2\sigma_8^2}} \,\mathrm{d}x. \tag{18}$$

Thus, the total BER without eavesdropping is:

$$p_{0\text{err}}(B,C) = p_{1\text{err}}(B,C) = \frac{1}{2}\text{erfc}\left(\frac{V_s}{2}\sqrt{\frac{\eta_2}{2\sigma_8^2}}\right). \tag{19}$$

Fig. 3 Beam splitter attack



4.2 Bob's Attack

Bob owns the information about the squeezed state he prepared, but he does not own the state carrying the secret. If Bob is dishonest, his main goal is to intercept the quantum channel from Alice to Charlie. Generally, Bob employs a beam splitter attack on a_5 as shown in Fig. 3.

$$a'_B = \sqrt{\eta_2}a_{\mathrm{N2}} - \sqrt{1-\eta_2}a_5, \tag{20}$$

When Alice publishes the results x_{u}, p_{u} of the joint Bell measurement, Bob applies another unitary operation $D(-\sqrt{2(1-\eta_2)}(x_{\mathrm{u}} + \mathrm{i}p_{\mathrm{u}}))$ on a'_B, and then he can easily remove the noise added by him and obtain the state a_B. Utilizing his random bits string n_B, Bob can choose the right measurement basis to measure a_B. Suppose Alice sent bit 0 and Bob prepared an amplitude squeezed state, then Bob's result is:

$$x_{\mathrm{B}} = -\sqrt{(1-\eta_2)}x_3 + \sqrt{\eta_1(1-\eta_2)}e^{-r_1}A + \sqrt{\eta_2}x_{\mathrm{N2}} + \sqrt{2(1-\eta_2)}e^{-r_2}x_{\mathrm{in2}}(0). \tag{21}$$

Making use of Eqs. (8), (10) and (11), one can see that: $x_B \sim N(-\sqrt{1-\eta_2}B, \sigma_B^2)$, $\sigma_B^2 = 1 + \eta_1(1-\eta_2)(e^{-2r_1} - 1) + 2(1-\eta_2)e^{-2r_2}$. Thus Bob sets his judgment threshold as $-\sqrt{1-\eta_2}(B + \frac{V_s}{2})$. If Bob gets $x_B > -\sqrt{1-\eta_2}(B + \frac{V_s}{2})$, he demodulates a_{B} and obtains the right bit 0; or else he obtains the wrong bit 1, then the BER under Bob's attack is:

$$p_{0\mathrm{err}}(B) = p_{1\mathrm{err}}(B) = \frac{1}{2}\mathrm{erfc}\left(\frac{V_s}{2}\sqrt{\frac{1-\eta_2}{2\sigma_B^2}}\right). \tag{22}$$

4.3 Charlie's Attack

Charlie owns the state carrying the secret, however, he does not know the initial information about the squeezed state prepared by Bob. If Charlie is dishonest, his main goal is to intercept the quantum channel from Bob to Alice. Since the amplitude and the phase of Bob's squeezed states are all Gaussian variables, even Charlie applies the beam splitter attack like Bob; he can either get no information about the squeezed states. Therefore, his main method is to measure his quantum state directly. Suppose Alice sent bit 0 and Bob prepared an amplitude squeezed state, then Charlie has 50 % chance to choose the right component:

$$x_{CR} = x_7, \tag{23}$$

From Eq. (15), one can see: $x_{CR} \sim N(\sqrt{\eta_2}B + \sqrt{\eta_1\eta_2}A, \sigma_{CR}^2)$, $\sigma_{CR}^2 = 1 + \eta_1\eta_2(e^{-2r_1} - 1) + 2\eta_2 e^{-2r_2}$. As Charlie has no information about Bob's state, he can only set his judgment threshold as $\sqrt{\eta_2}(B + \frac{V_s}{2})$ that Alice publishes. Thus the total BERs of bits 0 and 1 are:

$$p_{0\mathrm{err}}(CR) = \frac{1}{2}\mathrm{erfc}\left(\frac{(V_s - 2A\sqrt{\eta_1})}{2}\sqrt{\frac{\eta_2}{2\sigma_{CR}^2}}\right), \tag{24}$$

$$p_{1\mathrm{err}}(CR) = \frac{1}{2}\mathrm{erfc}\left(\frac{(V_s + 2A\sqrt{\eta_1})}{2}\sqrt{\frac{\eta_2}{2\sigma_{CR}^2}}\right). \tag{25}$$

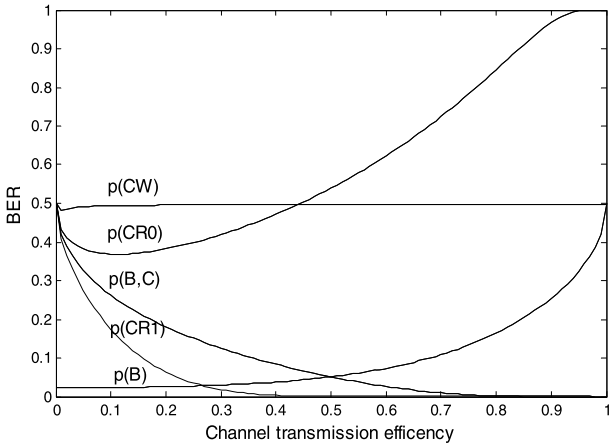


Fig. 4 The BER curve ($r_1 = 6$, $r_2 = 3$)

While Charlie also has 50 % chance to choose the wrong component:

$$p_{0\text{err}}(CW) = p_{1\text{err}}(CW) = \frac{1}{2}\text{erfc}\left(\frac{V_s}{2}\sqrt{\frac{\eta_2}{2\sigma_{CW}^2}}\right), \tag{26}$$

where $\sigma_{CW}^2 = 1 + \eta_1\eta_2(e^{2r_1} - 1) + 2\eta_2 e^{-2r_2}$.

4.4 Security Based on the BER

As analyzed above, four variables will affect the BER: the squeezed parameters r_1, r_2 and the quantum channel transmission efficiencies η_1, η_2. As e^{-r_1} and e^{-r_2} are always less than 1 when $r_1 > 0$, $r_2 > 0$, r_1 and r_2 can not play a dominant role and the BER can also be low even r_1, r_2 are finite. Thus, we just set $r_1 = 6$ and $r_2 = 3$ since other finite r_1, r_2 are also applicable in our analysis. Suppose $\eta_1 = \eta_2 = \eta$, that is to say, the two quantum channels are in a same environment. Figure 4 plots the BERs of every situations analyzed above, where p(CR0) and p(CR1) denote $p_{0\text{err}}(CR)$ and $p_{1\text{err}}(CR)$, respectively. It is shown that the BER decreases with the increment of the channel transmission efficiency if Bob and Charlie cooperate, and that the CVQSS scheme can work well only under a low squeezing degree and it does not need infinite squeezing since the BER is close to 0 at $\eta = 0.8$. If Bob is dishonest, the BER increases with the increment of the channel transmission efficiency and exceeds the case that Bob and Charlie cooperate when $\eta > 0.5$. Under binary bit modulation, the information between the communication parties is: $I = 1 + p\log_2 p + (1 - p)\log_2(1 - p)$, where p is the BER in the binary bit modulation. Then the information Bob eavesdropped is less than that Bob and Charlie cooperated when $\eta > 0.5$, which indicates that the scheme is secure to Bob when $\eta > 0.5$. If Charlie is dishonest, he will measure his state without the help of Bob. When he chooses the right component, the BER of bit 0 is close to 1, while the BER of bit 1 is close to 0. Apparently, Charlie can get nothing under this situation. If Charlie chooses the wrong component, the BER is close to 0.5, then the information Charlie eavesdropped is close to 0. Thus Charlie can get no information about the secret whatever he chooses the right component or the wrong one. In conclusion, when $\eta > 0.5$, the CVQSS scheme is secure to the dishonest participant, so it is also secure to the external eavesdropping.

In particular, suppose that Bob and Charlie are actually the same party (the same person). In this case, our proposed scheme reduces to a standard quantum key distribution protocol (between Alice and only one other party) with continuous variables. Compared with the

previous quantum key distribution protocols, the proposed CVQSS scheme has some advantages. The schemes in Refs. [26, 27] need the receivers randomly to choose and measure one of the two quadratures, but the receivers always do not know which component implied the key bit, then only half of the states can be used to generate key bits. If Bob and Charlie are the same person in the CVQSS scheme, Bob can always measure the right component, therefore the utilization of the quantum states in the CVQSS scheme are twice as that in Refs. [26, 27]. On the other hand, the BER in Ref. [28] is 4.8 % under ideal situations ($\eta = 1$), while the CVQSS scheme can achieve a lower BER just at $\eta = 0.8$. Therefore, the proposed scheme can also be used to transmit the secret to one party efficiently under nonideal conditions.

5 Conclusion

The DVQSS schemes will be difficult to meet the vast demands of future communications, while the QSS schemes based on continuous variables have a higher channel capacity. Unlike most of the existing continuous variable QSS schemes that sharing a quantum states finally, we propose a CVQSS scheme with finite squeezing to share classical secret keys directly. The participant Bob prepares and sends a squeezed states to Alice, then Alice encodes her bits on the squeezed states and sends them to another participant Charlie via quantum teleportation. Bob and Charlie can rebuild the classical secret keys when they cooperate. The security of the CVQSS scheme is analyzed in detail with BERs under different situations. When $\eta > 0.5$, neither Bob nor Charlie can get the secret alone without being detected. The CVQSS scheme can securely and effectively share secret messages with dishonest participants.

Acknowledgements This work is supported by the National Natural Science Foundation of China (grant no. 10647133), the Natural Science Foundation of Jiangxi Province, China (grant no. 20122BAB201031), the Foundation for Young Scientists of Jiangxi Province (Jinggang Star) (grant no. 20122BCB23002) and the Research Foundation of the Education Department of Jiangxi Province (grant no. GJJ13057).

References

1. Zeng, G.H., Wang, X.M.: China Inf. Secur. **78**, 1 (1999)
2. Hillery, M., Buzek, V., Berthiaume, A.: Phys. Rev. A **59**, 1829 (1999)
3. Cleve, R., Gottesman, D., Lo, H.K.: Phys. Rev. Lett. **83**, 648 (1999)
4. Gottesman, D.: Phys. Rev. A **61**, 042311 (2001)
5. Imai, H., Nascimento, A.C.A., Mueller-Quade, J.: Phys. Rev. A **64**, 042311 (2001)
6. Li, L.Z., Qiu, D.W., Mateus, P.: J. Phys. A, Math. Theor. **46**, 045304 (2013)
7. Xiao, L., Long, G.L., Deng, F.G., Pan, J.W.: Phys. Rev. A **69**, 052307 (2004)
8. Li, Y.M., Zhang, K.S., Peng, K.C.: Phys. Lett. A **324**, 420 (2004)
9. Deng, F.G., Li, X.H., Zhou, H.Y., Zhang, Z.: Phys. Rev. A **72**, 044302 (2005)
10. Takesue, H., Inoue, K.: Phys. Rev. A **74**, 012315 (2006)
11. Han, L.F., Liu, Y.M., Liu, J., Zhang, Z.J.: Opt. Commun. **281**, 2690 (2008)
12. Huang, D.Z., Chen, Z.G., Guo, Y.: Commun. Theor. Phys. **51**, 221 (2009)
13. Sarvepalli, P.: Phys. Rev. A **83**, 042324 (2011)
14. Jia, H.Y., Wen, Q.Y., Gao, F., Qin, S.J., Guo, F.Z.: Phys. Lett. A **376**, 1035 (2012)
15. Du, R.G., Sun, Z.W., Wang, B.H., Long, D.Y.: Int. J. Theor. Phys. **51**, 2727 (2012)
16. Tsai, C.W., Yang, C.W., Hwang, T.: Quantum Inf. Process. **11**, 113 (2012)
17. Tittel, W., Zbinden, H., Gisin, N.: Phys. Rev. A **63**, 042301 (2001)
18. Lance, A.M., Symul, T., Bowen, W.P., Sanders, B.C., Lam, P.K.: Phys. Rev. Lett. **92**, 177903 (2004)
19. Tyc, T., Sanders, B.C.: Phys. Rev. A **65**, 042310 (2002)
20. Lance, A.M., Symul, T., Bowen, W.P., Tyc, T., Sanders, B.C., Lam, P.K.: New J. Phys. **5**, 304 (2003)

21. Lance, A.M., Symul, T., Bowen, W.P., Sanders, B.C., Tyc, T., Ralph, T.C., Lam, P.K.: Phys. Rev. A **71**, 033814 (2005)
22. Zhang, J.X., Jing, J.T., Xie, C.D., Chin, P.K.C.: Phys. Lett. **22**, 2751 (2005)
23. Furusawa, A., Takei, N.: Phys. Rev. **443**, 97 (2007)
24. Takei, N., Yonezawa, H., Aoki, T., Furusawa, A.: Phys. Rev. Lett. **94**, 220502 (2005)
25. Qin, S.J., Gao, F., Wen, Q.Y., Zhu, F.C.: Phys. Lett. A **357**, 101 (2006)
26. Cerf, N.J., Levy, M., Assche, G.V.: Phys. Rev. A **63**, 052311 (2001)
27. Grosshans, F., Grangier, P.: Phys. Rev. Lett. **88**, 057902 (2002)
28. Li, Y.M., Zhang, K.S., Xie, C.D.: Acta Sinica Quantum Optica **8**, 71 (2002)