Mathematical Biosciences and Engineering

http://www.aimspress.com/journal/MBE

MBE, 16(5): 4182–4195.
DOI: 10.3934/mbe.2019208
Received: 06 January 2019
Accepted: 04 April 2019
Published: 13 May 2019

*Research article*

# Continuous variable quantum steganography protocol based on quantum identity

**Zhiguo Qu[1,*], Leiming Jiang[2], Le Sun[1], Mingming Wang[3] and Xiaojun Wang[4]**

[1] Jiangsu Collaborative Innovation Center of Atmospheric Environment and Equipment Technology (CICAEET), Nanjing University of Information Science & Technology, Nanjing, 210044, P. R. China

[2] School of Electronic & Information Engineering, Nanjing University of Information Science and Technology, Nanjing 210044, P. R. China

[3] School of Computer Science, Xi'an Polytechnic University, Xi'an 710048, P. R. China

[4] School of Electronic Engineering, Dublin City University, Dublin, Ireland

* **Correspondence:** Email: qzghhh@126.com; Tel: +86-15895923386.

**Abstract:** Based on quantum identity authentication, a novel continuous variable quantum steganography protocol is proposed in this paper. It can effectively transmit deterministic secret information in the public quantum channel by taking full advantage of entanglement properties of continuous variable GHZ state. Compared with the existing quantum steganography results, this protocol has the advantages of good imperceptibility and easy implementation. Finally, the detailed performance analysis proves that the proposed protocol has not only these advantages, but also good security and information transmission efficiency, even under eavesdropping attacks, especially to the spectroscopic noise attack.

**Keywords:** quantum steganography; continuous variable GHZ state; spectroscopic noise attack

## 1. Introduction

Compared with classical information hiding, quantum information hiding has unparalleled advantages based on the non-cloning theorem, uncertainty principle, quantum non-locality, such as good security and high information transmission efficiency. Since Bennett and Brassard proposed the first quantum cryptography communication protocol in 1984 [1], many quantum cryptographic communication protocols such as quantum key distribution (QKD) [2–4], quantum identity authentication (QIA) [5], quantum secrets sharing (QSS) [6–8] and quantum security direct communications (QSDC) [9,10] have emerged. In recent years, the theoretical research and application of quantum communication has been developed in a variety of ways, including quantum computation [11], quantum remote state preparation [12–14], quantum network coding [15,16], quantum auction [17] and quantum machine learning [18,19].

Among them, quantum steganography, as a research branch of quantum information hiding, aims at covertly transmitting secret information in public quantum channel. Usually, it can be mainly divided into two categories. The first one is to use quantum communication characteristics to perform covert communication through single-particle or multi-particle as quantum carriers [20–22]. In 2018, Zhu et al. proposed a novel quantum steganography protocol based on Brown entangled states, which proved its good security resisting on quantum noise [23]. The second is to embed secret information into various multimedia carriers for covert communication [24,25]. In 2018, Qu et al. proposed a novel quantum image steganography algorithm based on exploiting modification direction [26].

So far, most of the previous quantum steganography protocols are mainly based on discrete variables. Recently, the continuous variable quantum communication technique is beginning to emerge [27]. It uses a classical light source as a signal source, and can encode information on a continuously changing observable physical quantity with low cost due to easy implementation. The encoded information is a symbol, which can be restored to binary bits only after some specific data processing. Therefore, the capacity of this technique can be large and the key generation rate is also high, which has quickly attracted widespread attention. As an example, the continuous-variable quantum key distribution (CVQKD) has absolute advantages over the discrete-variable quantum key distribution (DVQKD). The detection of DVQKD is based on single photons. The single photon signal is not only difficult to manufacture, but also difficult to be detected and costly. The CVQKD is using homodyne/heterodyne decoding to obtain quadrature encoding, which greatly improves the technical efficiency. In addition, non-Gaussian operations have many applications in improving the quantum entanglement and teleportation. In 2003, Olivares et al. proposed the Inconclusive photon subtraction (IPS) to improve teleportation [28]. In 2015, Wu et al. applied local coherent superposition of photon subtraction and addition to each mode of even entangled coherent state to introduce a new entangled quantum state [29]. In 2018, the CVQKD with non-Gaussian quantum catalysis was proposed [30].

In this paper, a continuous variable quantum steganography protocol is proposed based on the continuous variable GHZ entangled state [31] and the continuous variable quamtum identity authentication protocol [32]. The protocol can realize the transmission of deterministic secret information in public quantum channel of identity authentication. It can convert segmented secret information into the whole secret information by adopting the specific encoding rule, randomly selecting quantum channel and replacing time slot. Through effectively verifying the identity of users, in the new protocol, the secret information can be implicitly transmitted to the recipient Bob, while the eavesdropper Eve disables to detect the existence of covert communication. Compared with the previous quantum steganography protocols, by introducing continuous variables into quantum steganography and making full use its characteristics of continuous variable, the proposed protocol can obtain the advantages of good imperceptibility, security and easy implementation for good applicability.

The paper is organized as follows. Section 2 introduces some basic knowledge about optics, the preparation of continuous variable GHZ states, and the principle of continuous variable quantum telecommuting required for the identity authentication process. Section 3 describes the concrete steps of the new continuous variable quantum steganography protocol in detail. Section 4 mainly analyzes the new protocol's imperceptibility, security and efficiency of information transmission, even in quantum noise environment. The conclusions are given in Section 5.

## 2. Preliminary

### 2.1. Quantum continuous variable and its encoding rules

We first review some of the knowledge of quantum optics. By using the creation operator $a^{\dagger}$ and the annihilation operator $a$, the two regular components including the amplitude x and the phase p of a beam can be expressed as

$$x = \frac{1}{2}\left(a^{\dagger} + a\right) \tag{2.1}$$

$$p = \frac{i}{2}\left(a^{\dagger} - a\right) \tag{2.2}$$

where $a^{\dagger}$ and $a$ satisfy boson reciprocity $[a, a] = \left[a^{\dagger}, a^{\dagger}\right] = 0$, $\left[a, a^{\dagger}\right] = 1$. Therefore $[x, p] = \frac{i}{2}$, two typical components x and p satisfy the Heisenberg uncertainty principle: $\Delta x \cdot \Delta p \geq \frac{1}{4}$.

A squeezed beam can be defined as

$$|\alpha, r\rangle = x + ip = e^{r} x(0) + ie^{-r} p(0) \tag{2.3}$$

where $r$ is the compression factor. If $r < 0$, it indicates that the beam amplitude is compressed; if $r > 0$, it indicates that the beam phase is compressed. $x(0)$ and $p(0)$ indicate the amplitude and the phase of the vacuum state respectively, and $x(0), p(0) \sim N\left(0, \frac{1}{4}\right)$.

In the proposed protocol, the legal communication parties share the encoding rule in advance. They can encode the discrete information into different intervals(Turbo codes [33] or LDPC code [34]).

### 2.2. Preparation of continuous variable GHZ state

The continuous variable GHZ state is very important for quantum information processing and quantum communication in the new protocol. As shown in Figure 1, the continuous variable GHZ state is produced by making two squeezed vacuum states $a_{in1}$ and $a_{in2}$ pass through a beam splitter $BS_1$ (transmission coefficient is 0.5) to generate $a_{out1}$ and $a^{*}_{in3}$ firstly. And then, it makes $a^{*}_{in3}$ and another squeezed vacuum state $a_{in3}$ pass through a beam splitter $BS_2$ (transmission coefficient is 1) to generate $a_{out2}$ and $a_{out3}$. Obviously, $a_{out1}$, $a_{out2}$ and $a_{out3}$ is a set of the continuous variable GHZ entangled state that be defined as

$$x_{out1} = \frac{1}{\sqrt{3}} e^{r_1} x_{in1}(0) + \sqrt{\frac{2}{3}} e^{-r_2} x_{in2}(0) \tag{2.4}$$

$$p_{out1} = \frac{1}{\sqrt{3}} e^{-r_1} p_{in1}(0) + \sqrt{\frac{2}{3}} e^{r_2} p_{in2}(0) \tag{2.5}$$

$$x_{out2} = \frac{1}{\sqrt{3}} e^{r_1} x_{in1}(0) - \frac{1}{\sqrt{6}} e^{-r_2} x_{in2}(0) + \frac{1}{\sqrt{2}} e^{-r_3} x_{in3}(0) \tag{2.6}$$

$$p_{out2} = \frac{1}{\sqrt{3}}e^{-r_1}p_{in1}(0) - \frac{1}{\sqrt{6}}e^{r_2}p_{in2}(0) + \frac{1}{\sqrt{2}}e^{r_3}p_{in3}(0) \tag{2.7}$$

$$x_{out3} = \frac{1}{\sqrt{3}}e^{r_1}x_{in1}(0) - \frac{1}{\sqrt{6}}e^{-r_2}x_{in2}(0) - \frac{1}{\sqrt{2}}e^{-r_3}x_{in3}(0) \tag{2.8}$$

$$p_{out3} = \frac{1}{\sqrt{3}}e^{-r_1}p_{in1}(0) - \frac{1}{\sqrt{6}}e^{r_2}p_{in2}(0) - \frac{1}{\sqrt{2}}e^{r_3}p_{in3}(0) \tag{2.9}$$

Let suppose that $r_1 = r_2 = r_3 = r$, it can calculate the correlation of amplitude and phase between $a_{out1}$, $a_{out2}$ and $a_{out3}$

$$\left\langle [\Delta(x_{out1} - x_{out2})]^2 \right\rangle = \left(\frac{1}{2} - \frac{\sqrt{3}}{4}\right)e^{-2r} \tag{2.10}$$

$$\left\langle [\Delta(x_{out1} - x_{out3})]^2 \right\rangle = \left(\frac{1}{2} + \frac{\sqrt{3}}{4}\right)e^{-2r} \tag{2.11}$$

$$\left\langle [\Delta(p_{out1} + p_{out2} + p_{out3})]^2 \right\rangle = \frac{3}{4}e^{-2r} \tag{2.12}$$

If the compression parameter $r \to +\infty$, the correlation between the output optical modes $a_{out1}$, $a_{out2}$ and $a_{out3}$ will become stronger and stronger

$$\lim_{r\to+\infty}(x_{out1} - x_{out2}) = \lim_{r\to+\infty}(x_{out1} - x_{out3}) = 0 \tag{2.13}$$

$$\lim_{r\to+\infty}(p_{out1} + p_{out2} + p_{out3}) = 0 \tag{2.14}$$

It is obvious that the amplitude between any two of the continuous variable GHZ state output modes is positively correlated, and the phase between them also has the entanglement characteristic.

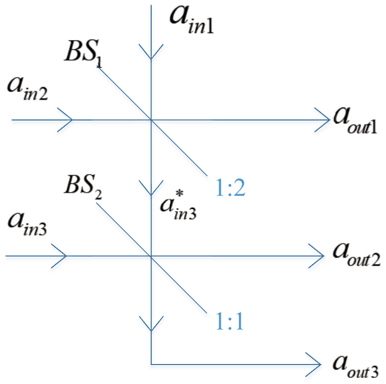

**Figure 1.** Preparation of continuous variable GHZ state.

### *2.3. The principle of continuous variable quantum telecommuting*

The principle of continuous variable quantum telecommuting can be described as shown in Figure 2. Alice prepares a coherent state $a_A = |x_A + ip_A\rangle$ to be transmitted. Simultaneously, Alice and Bob share two entangled optical modes $a_{out1}$ and $a_{out2}$. After everything is ready, Alice sends the coherent state and $a_{out1}$ through a 50/50 beam splitter for Bell state measurement to obtain $x_o$ and $p_o$

$$x_o = \frac{1}{\sqrt{2}}(x_A - x_{out1}) \tag{2.15}$$

$$p_o = \frac{1}{\sqrt{2}}(p_A + p_{out1}) \tag{2.16}$$

After Alice announces the measurement results through the classic channel, Bob takes the corresponding unitary operation $D\left(\beta = \sqrt{2}\,(x_o + ip_o)\right)$ on $a_{out2}$ to obtain

$$x_B = x_{out2} + \sqrt{2}x_o = x_A - (x_{out1} - x_{out2}) \tag{2.17}$$

$$p_B = p_{out2} + \sqrt{2}p_o = p_A + (p_{out1} + p_{out2}) \tag{2.18}$$

According to Eqs. (2.13) and (2.14), if the compressing parameter $r \to +\infty$, we can obtain $x_B = x_A$, $p_B = p_A - p_{out3}$. It means that Alice and Bob obtain a highly correlated sequence on the amplitude component. Therefore, in the proposed protocol, we only modulate the effective information on the amplitude component and the uncorrelated random information $n$ on the phase component.

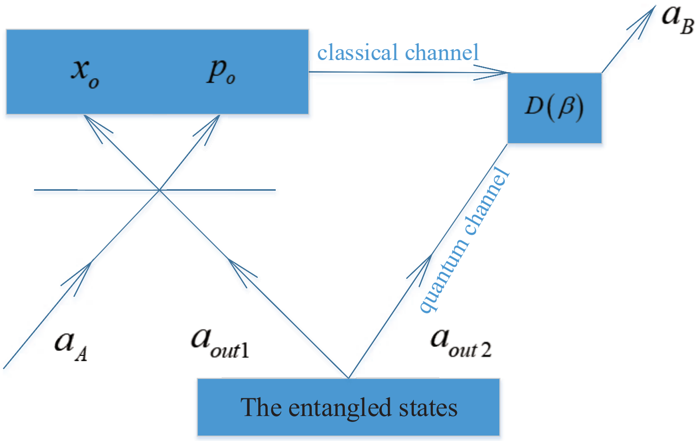

**Figure 2.** The principle of continuous variable quantum telecommuting.

## 3. Continuous variable quantum steganography protocol

We propose a novel continuous variable quantum steganography protocol based on quantum identity authentication protocol and continuous variable GHZ state. It can effectively transmit deterministic secret information in the public quantum channel. When Bob attempts to communicate with Alice, they need to share an initial identity key $K_1$ and a series of time slot keys $T$ which are binary sequences known only to Alice and Bob in advance.

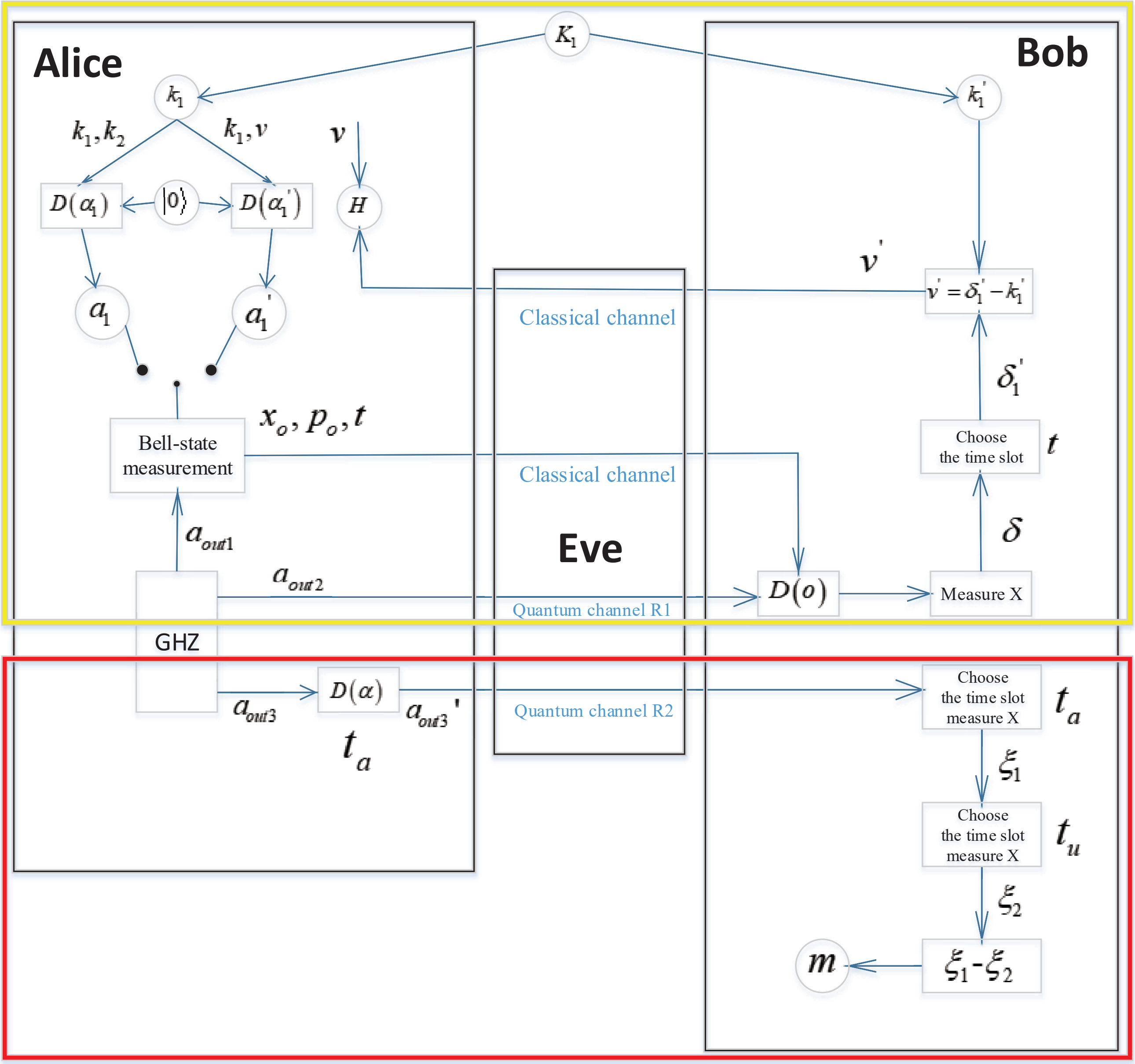

**Figure 3.** Continuous variable quantum steganography protocol.

Here, $D(\alpha)$, $D(\alpha_1)$ and $D(\alpha_1{}')$ are the displacement operation; $D(o)$ is the unitary operation, and $H$ is the fidelity parameter. The yellow area represents the normal information transmission mode. The red area represents the secret information transmission mode.

The details of the protocol are shown in Figure 3. We assume that the quantum channel is lossless, the proposed protocol is as follows.

Alice prepares the continuous variable GHZ entangled states $a_{out1}$, $a_{out2}$ and $a_{out3}$. Alice keeps $a_{out1}$ by herself, then transmits $a_{out2}$ and $a_{out3}$ to Bob through two quantum channels R1 and R2 respectively. Alice randomly selects a quantum channel for normal information transmission mode (identity authentication). The other is the channel of the secret information transmission mode (steganographic information).

The normal information transmission mode:

(A1) Alice chooses $a_{out2}$ (R1 channel) or $a_{out3}$ (R2 channel) to send to Bob. For convenience, we assume that the channel selected by the normal information transmission mode is the R1 channel.

(A2) After Alice confirms that Bob has received $a_{out2}$, she converts $K_1$ to decimal sequence $k_1$. And then, Alice selects two decimal numbers $k_2$ and $v$, satisfying the normal distribution $N\left(0, \sigma^2\right)$. Alice prepares a vacuum state $|0\rangle$ with displacement operation $D\left(\alpha_1 = (k_1 + k_2) + in\right)$. The coherent state optical mode $a_1$ which is used to update the identity key, is obtained. Simultaneously, Alice also prepares a vacuum state with displacement operation $D\left(\alpha_1{}' = (k_1 + v) + in\right)$. The coherent state optical mode $a_1{}'$, which is used as a decoy state for identity authentication, is obtained. After that, Alice randomly selects $a_1$ or $a_1{}'$ to make Bell state measurement with $a_{out1}$ on each time slot and obtains, $x_o = \frac{1}{\sqrt{2}}(x_1 - x_{out1})$ and $p_o = \frac{1}{\sqrt{2}}(p_1 + p_{out1})$, or $x_o = \frac{1}{\sqrt{2}}(x_1{}' - x_{out1})$ and $p_o = \frac{1}{\sqrt{2}}(p_1{}' + p_{out1})$. Then, Alice announces $x_o$ and $p_o$ to Bob through the public classic channel.

(A3) According to the received $x_o$ and $p_o$, Bob performs the unitary operation $D\left(o = \sqrt{2}\,(x_o + ip_o)\right)$ on the received $a_{out2}$, and then selects the amplitude component to measure and get the sequence $\delta$. Alice publishes the time slots $t$ which used $a_1{}'$, and Bob measures the amplitude components on these time slots to obtain a sequence $\delta_1{}'$. The value of sequence $\delta$ minus sequence $\delta_1{}'$ is defined as $\delta_1$.

(A4) Bob converts $K_1$ to a decimal sequence $k_1{}'$, then calculates $v' = \delta_1{}' - k_1{}'$. After Bob announces $v'$, Alice calculates a fidelity parameter $H = \left\langle [v' - \varphi v]^2 \right\rangle_{\min}$. In the lossless channel, we get $\varphi$=1. If the calculation $H$ is equal to 0, it means $k_1 = k_1{}'$. The user identity is verified to be legal. Bob then updates the identity key sequence $\delta_1 - k_1{}'$ to obtain $k_2$. If $H$ is greater than 0, it means that the eavesdropper Eve exists or the user is illegal. As a result, the communication will be abandoned.

The secret information transmission mode:

(B1) Alice divides her steganographic information into p-blocks for block transmission. Let assume that the steganographic information of the q-th block ($q \leq p$) is 010. According to the previously shared encoding rule, steganographic information 010 corresponds to the interval $(-2, -1]$. After that, Alice takes the first time slot $T_a$ from the binary time slot key $T$ and converts it to a decimal number $t_a$. And then, she chooses the random variable $m \in (-2, -1]$, and does the translation operation $D\,(\alpha = m + in)$ on $a_{out3}$ in the time slot $t_a$ to get $a_{out3}{}'$, where $m$ is the secret information that needs to be transmitted. Alice sends $a_{out3}{}'$ to Bob via quantum channel R2.

(B2) Bob also obtains $t_a$ based on the shared time slot key, and measures the amplitude component of the received beam mode $a_{out3}{}'$ in the time slot $t_a$ to obtain the sequence $\xi_1$. After that, Bob then selects the time slot $t_u$ ($u \neq a$) to measure the amplitude component for obtaining the sequence $\xi_2$. Bob calculates $\xi_1 - \xi_2$ to obtain the secret information $m$.

(B3) According to the previously shared encoding rule, the information of the q-th block is obtained by Bob. The identity keys of both parties are also updated, and the transmission of the secret information of this block is completed. In the next round, Alice randomly selects one quantum channel for normal information transmission mode, and another quantum channel for secret information transmission mode. Then Alice repeats the above steps until all the steganographic information are transmitted.

As shown in Figure 3, when Alice wants to transmit private information to Bob, she randomly selects a quantum channel for identity authentication by using the modulated vacuum states and the continuous variable quantum telecommuting. At the same time, after the encoded secret information is modulated in the shared time slot, the transmission of the secret information is also carried out in another quantum channel. Under the cover of determining whether the Bob's identity is legal, it is difficult for an eavesdropper to discover that another channel is transmitting information. Even if the eavesdropper knows the existence of the secret information, it is impossible to obtain useful information without knowing the modulated time slot and the encoding rule.

In the field of experiment, the protocol is also feasible. The secure transmission using entangled squeezed states has been exemplified [35]. The experimental demonstration of the continuous variable quantum telecommuting has also been proposed [36]. Our protocol is mainly based on these two techniques. Therefore, this protocol is capable of having good performance in experiments.

## 4. Security analysis

The security of the scheme is mainly based on the entanglement properties of the GHZ state, the specific encoding rule, the shared time slot key and the block transmission. Among them, quantum entanglement guarantees the correlation of quantum transmission. The encoding rule ensures that the information in the quantum channel is not completely equal to the identity key information. The shared time slot key decides the writing and reading of the secret information.

The normal message transmission mode is to avoid Eve's active attack through identity authentication. In order to conduct an active attack, Eve needs to be authenticated. The most effective method is to obtain an updated authentication key and implement an active attack in the next authentication flow. In order to obtain the updated authentication key, Eve's good optional method is to intercept all the quantum signals sent by Alice and measure their components. Combined with the information sent by the classic channel, Eve can recover the updated authentication key and prepare a quantum state to send to Bob during an authentication process. However, due to the quantum uncertainty principle, Eve will inevitably introduce excessive noise, which will be detected by the legal user through the calculation of the fidelity parameter. As shown in Figure 3, there are two quantum channels and two classical channels in the proposed protocol. We have always assumed that the information transmitted in the classical channel is public, and the security of the normal information transmission mode has been proved above [32]. Therefore, we focus on the security of the secret information transmission mode.

It's noteworthy that this protocol may suffer from physical attacks, such as the wavelength attack. This kind of attack makes full of use of the potential imperfections in the protocol's implementation to enable the eavesdropper to control the light intensity transmission of the receiver's splitter. The attack method is to intercept the beam and measure the signal using the local oscillator by heterodyne measurement to obtain the quadrature values, and then switch the wavelength of the input light. It can make the eavesdropper completely control the receiver's beam splitter without being discovered. In this case, the new protocol is also capable of resisting the attack by randomly adding or not adding a wavelength filter before the monitoring detector and observing the difference value [37].

Because only two quantum channels (R1 and R2) are used to transmit quantum information and the information is modulated on the amplitude and phase of the beam, the attacker Eve can take an attack by using a spectroscope to intercept the signal for measurement and attempting to obtain the key. As shown in Figure 4, Let assume that the spectroscopic coefficient used by Eve is $\gamma\,(0 \leq \gamma \leq 1)$. The two beams $a_{A1}$ and $a_{A2}$ sent by Alice pass through the beam splitter and become

$$a_{B1} = \sqrt{\gamma}a_{A1} + \sqrt{1-\gamma}a_{N1} \tag{4.1}$$

$$a_{B2} = \sqrt{\gamma}a_{A2} + \sqrt{1-\gamma}a_{N2} \tag{4.2}$$

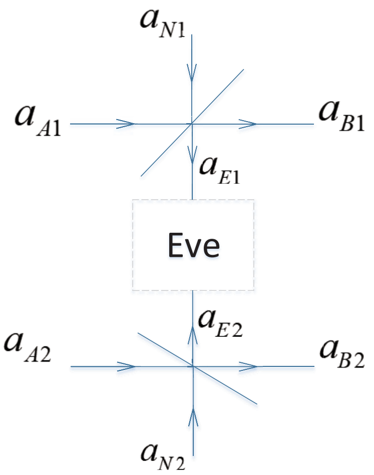

**Figure 4.** The spectroscopic noise attack.

Eve can obtain $a_{E1}$ and $a_{E2}$

$$a_{E1} = \sqrt{\gamma}a_{N1} - \sqrt{1-\gamma}a_{A1} \tag{4.3}$$

$$a_{E2} = \sqrt{\gamma}a_{N2} - \sqrt{1-\gamma}a_{A2} \tag{4.4}$$

According to the difference of the spectroscopic coefficients, the safety analysis can be carried out in three cases:

1. If $\gamma = 0$, Eve intercepts all signals. In this case, Eve may combine $a_{E1}$ and $a_{E2}$ with the Bell state measurement to obtain

$$x_u = \frac{1}{\sqrt{2}}(x_{E1} - x_{E2}) = \frac{1}{\sqrt{2}}(x_{A1} - x_{A2}) \tag{4.5}$$

$$p_u = \frac{1}{\sqrt{2}}(p_{E1} + p_{E2}) = \frac{1}{\sqrt{2}}(p_{A1} + p_{A2}) \tag{4.6}$$

Due to the correlation between the amplitudes of $a_{A1}$ and $a_{A2}$, Eve measures the amplitude component, as $x_u \rightarrow 0$. Even if the time slot containing the secret information has been stolen, Eve disables to get any information. The phase of $a_{A1}$ and $a_{A2}$ does not modulate the secret information, and only the uncorrelated random information $n$ exists. Therefore, Eve will only think that it is the ordinary noise in the quantum channel, so that the transmission of the secret information can be undetected.

Eve may also measure $a_{A1}$ and $a_{A2}$ separately. According to the principle of key modulation, let assume that Eve measures the amplitude of $a_{A1}$ and the phase of $a_{A2}$ respectively. Because the correlation of amplitude, Eve can recover $a_{A2}$ after measurement. However, due to the quantum uncertainty principle, Eve cannot recover the phase of $a_{A1}$ and this operation will reduce the phase entanglement of the GHZ state. It will inevitably be detected by performing eavesdropping detection from legitimate parties.

It can be seen that Eve's eavesdropping will be detected by legitimate parties, and this protocol can safely transmit secret information when $\gamma = 0$.

2. If $\gamma$= 1, Eve does not take any action, obviously cannot get any information.

3. When $0 \leq \gamma \leq 1$, Eve only intercepts part of the signal, and another part of the signal is still transmitted to the receiver.

In this case, due to the entanglement properties of the GHZ state, Eve cannot obtain effective information with the Bell state measurement, so Eve can only operate on $a_{E1}$ and $a_{E2}$ separately. Because the secret information is modulated on one of the quantum channels, let choose $a_{E1}$ to analyze it as an example. Let Assume that the quantum channel transmission efficiency is $\lambda$, the signal received by Bob will be

$$a_{B1} = \sqrt{\lambda} a_{A1} + \sqrt{1-\lambda} a_{N1} \tag{4.7}$$

Eve needs to amplify $a_{E1}$ to avoid being detected and sends it to Bob with $a_{B1}$. The effective signal received by Bob is

$$a = g a_{E1} + a_{B1} \tag{4.8}$$

Here, $g$ is the gain compensation. According to Eqs. (4.1), (4.3) and (4.8), in order to receive the signal $\sqrt{\lambda} a_{A1}$ for Bob, it needs to be satisfied with

$$\sqrt{\lambda} a_{A1} = -g\sqrt{1-\gamma} a_{A1} + \sqrt{\gamma} a_{A1} \tag{4.9}$$

Eve obtain $g = \frac{\sqrt{\gamma} - \sqrt{\lambda}}{\sqrt{1-\gamma}}$. Due to the information is modulated on the amplitude component , the noise signal received by Bob will be

$$a_N = \frac{1 - \sqrt{\lambda\gamma}}{\sqrt{1-\gamma}} x_{N1} \tag{4.10}$$

If $\gamma \neq \lambda$ and $a_N \neq \sqrt{1-\lambda} x_{N1}$, the signal-to-noise ratio received by Bob will change. The legitimate parties will find Eve in the eavesdropping detection. If $\gamma$=$\lambda$, $g$=0, it does not require the gain compensation. Eve will be undetected by the legitimate parties.

Therefore, if $0 \leq \gamma \leq 1$, Eve can adopt the best attack method is intercepting by a beam splitter with the same spectroscopic coefficient and channel transmission efficiency. The signal received by Eve will be

$$a_{E1} = \sqrt{\lambda} a_{N1} - \sqrt{1-\lambda} a_{A1} \tag{4.11}$$

The signal received by Bob is

$$a_{B1} = \sqrt{\lambda} a_{A1} + \sqrt{1-\lambda} a_{N1} \tag{4.12}$$

According to Eq. (2.6), the amplitude components of Eve and Bob are obtained as follows

$$x_{E1} = \sqrt{\lambda} x_{N1} - \sqrt{1-\lambda}\left[\frac{1}{\sqrt{3}} e^{r} x_{in1}(0) - \frac{1}{\sqrt{6}} e^{-r} x_{in2}(0) + \frac{1}{\sqrt{2}} e^{-r} x_{in3}(0)\right] \tag{4.13}$$

$$x_{B1} = \sqrt{\lambda}\left[\frac{1}{\sqrt{3}} e^{r} x_{in1}(0) - \frac{1}{\sqrt{6}} e^{-r} x_{in2}(0) + \frac{1}{\sqrt{2}} e^{-r} x_{in3}(0)\right] + \sqrt{1-\lambda} x_{N1} \tag{4.14}$$

Here, $x_{N1} \sim N(0, V_{N1})$. If we measure the amplitude of $a_{B1}$, only $\sqrt{\frac{\lambda}{3}}e^r x_1(0)$ will be the effective signal, while the rest are noise. The signal-to-noise ratio of Bob can be calculated as

$$\frac{M_{B1}}{N_{B1}} = \frac{\lambda e^{2r}}{2\lambda e^{-2r} + 12(1-\lambda)V_{N1}} \tag{4.15}$$

The amount of information between Alice and Bob is

$$I(A, B) = \frac{1}{2}\log_2\left(1 + \frac{M_{B1}}{N_{B1}}\right) \tag{4.16}$$

Similarly, the signal-to-noise ratio of Eve is

$$\frac{M_{E1}}{N_{E1}} = \frac{(1-\lambda)e^{2r}}{2(1-\lambda)e^{-2r} + 12\lambda V_{N1}} \tag{4.17}$$

The amount of information between Alice and Eve is

$$I(A, E) = \frac{1}{2}\log_2\left(1 + \frac{M_{E1}}{N_{E1}}\right) \tag{4.18}$$

Therefore, according to the Shannon information theory, the quantum channel transmission rate is

$$\Delta I = I(A, B) - I(A, E) = \frac{1}{2}\log_2\left(\frac{\lambda\left(e^{2r} + 2e^{-2r}\right) + 12(1-\lambda)V_{N1}}{2\lambda e^{-2r} + 12(1-\lambda)V_{N1}} \cdot \frac{2(1-\lambda)e^{-2r} + 12\lambda}{(1-\lambda)(e^{2r} + 2e^{-2r}) + 12\lambda V_{N1}}\right) \tag{4.19}$$

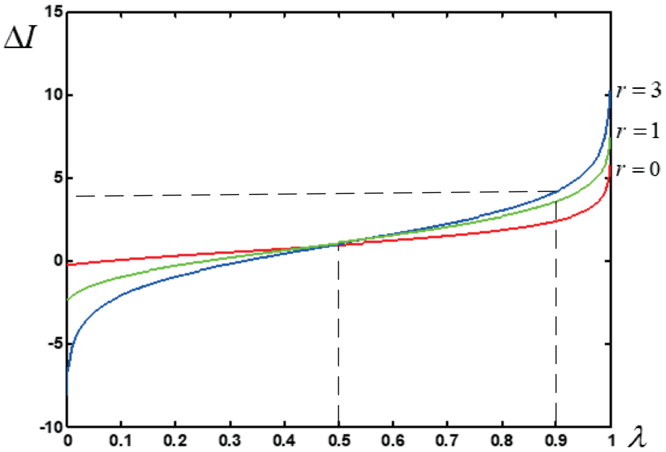

**Figure 5.** Secret information transmission rate ($V_{N1}=\frac{1}{4}$).

If $V_{N1}=\frac{1}{4}$, the secret information transmission rate obtained by Eq. (4.19) is as shown in Figure 5. The secret information transmission rate $\Delta I$ is proportional to the quantum channel transmission efficiency $\lambda$. If the channel transmission efficiency $\lambda < 0.5$, the information transmission rate $\Delta I < 0$, the amount of information acquired by Eve is greater than the amount of information obtained by Bob, so that the channel is unsafe. If the channel transmission efficiency $\lambda > 0.5$, the information transmission rate $\Delta I > 0$, the secret information transmission can be carried out safely. The security of the proposed protocol is also dependent on the entanglement properties of the continuous variable GHZ state. If the compression parameter $r = 0$, the information transmission rate will reach 0. It is almost impossible to transmit information. If the compression parameter $r$ increases, the information transmission rate also increases. Compared with discrete variable communication, it can also greatly reduce the quantum states that need to be prepared and shorten the time required for information transmission. For example, the discrete variables communication can only transmit 1 bit of classical information per qubit. If a deterministic key of 1000 bits is needed, at least 1000 qubits are required. In the proposed protocol, if $r = 3$ and the channel transmission efficiency is equal to 0.9, the information transmission rate will be 4 qubits/s. At this point, only 250 qubits is required to complete the same work. So it's obviously that the efficiency of information transmission can be greatly improved.

## 5. Conclusion

This paper proposes a novel continuous variable quantum steganography protocol based on quantum identity authentication. For covert communication, the protocol implements the transmission of secret information in public channel of quantum identity authentication. Compared with the existing quantum steganography results, by taking full advantage of entanglement properties of continuous variable GHZ state, this protocol not only has the advantages of good imperceptibility and easy implementation in physics, but also good security and information transmission efficiency, even under eavesdropping attacks especially to the spectroscopic noise attack. In addition, the capacity of secret information is potential to be enlarged by introducing better information coding method.

## Acknowledgments

This work was supported by the National Natural Science Foundation of China (No. 61373131, 61601358, 61501247, 61672290, 61303039, 61232016), the Six Talent Peaks Project of Jiangsu Province (Grant No. 2015-XXRJ-013), Natural Science Foundation of Jiangsu Province (Grant No. BK20171458), the Natural Science Foundation of the Higher Education Institutions of Jiangsu Province (China under Grant No.16KJB520030), Sichuan Youth Science and Technique Foundation (No.2017JQ0048), NUIST Research Foundation for Talented Scholars (2015r014), PAPD and CICAEET funds.

## Conflict of interest

The authors declare no conflict of interest.

## References

1. C. H. Bennett and G. Brassard, Quantum cryptography: public-key distribution and coin tossing, *Theor. Comput. Sci.*, **560** (2014), 7–11.
2. E. Diamanti, H. K. Lo and B. Qi, Practical challenges in quantum key distribution, *NPJ Quantum Inform.*, **2** (2017), 1–9.

3. M. Tomamichel and A. Leverrier, A largely self-contained and complete security proof for quantum key distribution, *Quantum*, **1** (2017), 14–23.
4. W. J. Liu, Y. Xu, C. N. Yang, et al., An efficient and secure arbitrary n-party quantum key agreement protocol using Bell states, *Int. J. Theor. Phys.*, **57** (2018), 195–207.
5. H. H. Chang, J. Heo and G. J. Jin, Quantum identity authentication with single photon, *Quantum Inf. Process.*, **16** (2017), 236–246.
6. A. Tavakoli, I. Herbauts and M. żukowski, Secret sharing with a single d-level quantum system, *Phys. Rev. A*, **92** (2015), 1–10.
7. C. M. Bai, Z. H. Li and T. T. Xu, Quantum secret sharing using the d-dimensional GHZ state, *Quantum Inf. Process.*, **16** (2017), 59–70.
8. X. B. Chen, X. Tang, G. Xu, et al., Cryptanalysis of secret sharing with a single d-level quantum system, *Quantum Inf. Process.*, **17** (2018), 225–235.
9. W. Li, J. Chen and X. Wang, Quantum secure direct communication achieved by using multi-entanglement, *Int. J. Theor. Phys.*, **54** (2015), 100–105.
10. J. Y. Hu, B. Yu and M. Y. Jing, Experimental quantum secure direct communication with single photons, *Light-SCI. Appl.*, **5** (2016), e16144.
11. W. J. Liu, Z. Y. Chen, J. S. Liu, et al., Full-blind delegating private quantum computation, *Comput. Mater. Con.*, **56** (2018), 211–223.
12. Z. G. Qu, S. Y. Wu, M. M. Wang, et al., Effect of quantum noise on deterministic remote state preparation of an arbitrary two-particle state via various quantum entangled channels, *Quantum Inf. Process.*, **16** (2017), 1–25.
13. X. B. Chen, Y. R. Sun, G. Xu, et al., Controlled bidirectional remote preparation of three-qubit state, *Quantum Inf. Process.*, **16** (2017), 244–254.
14. M. M. Wang, C. Yang and R. Mousoli, Controlled cyclic remote state preparation of arbitrary qubit states, *Comput. Mater. Con.*, **55** (2018), 321–329.
15. G. Xu, X. B. Chen and J. Li, Network coding for quantum cooperative multicast, *Quantum Inf. Process.*, **14** (2015), 4297–4307.
16. Z. G. Qu, J. Keeney, S. Robitzsch, et al., Multilevel pattern mining architecture for automatic network monitoring in heterogeneous wireless communication networks, *China. Commun.*, **13** (2016), 108–116.
17. W. J. Liu, H. B. Wang, G. L. Yuan, et al., Multiparty quantum sealed-bid auction using single photons as message carrier, *Quantum Inf. Process.*, **15** (2016), 869–879.
18. W. J. Liu, P. P. Gao, W. B. Yu, et al., Quantum Relief algorithm, *Quantum Inf. Process.*, **17** (2018), 280–290.
19. J. W. Wang, T. Li, X. Y. Luo, et al., Identifying computer generated images based on quaternion central moments in color quaternion wavelet domain, *IEEE T. Circ. Syst. Vid.*, (2018), online. DOI: 10.1109/TCSVT.2018.2867786.
20. L. Liu, G. M. Tang and Y. F. Sun, Quantum steganography for multi-party covert communication, *Int. J. Theor. Phys.*, **55** (2016), 1–11.

21. T. Mihara, Multi-party quantum steganography, *Int. J. Theor. Phys.*, **56** (2017), 1–8.
22. Z. G. Qu, S. Y. Chen, S. Ji, et al., Anti-noise bidirectional quantum steganography qrotocol with large payload, *Int. J. Theor. Phys.*, **57** (2018), 1–25.
23. Z. G. Qu, T. C. Zhu and J. W. Wang, A novel quantum steganography based on Brown states, *Comput. Mater. Con.*, **1** (2018), 47–59.
24. S. Wang, J. Sang and X. Song, Least significant qubit (LSQb) information hiding algorithm for quantum image, *Measurement*, **73** (2015), 352–359.
25. N. Jiang, N. Zhao and L. Wang, LSB based quantum image steganography algorithm, *Int. J. Theor. Phys.*, **55** (2016), 1–17.
26. Z. G. Qu, Z. W. Cheng, W. J. Liu, et al., A novel quantum image steganography algorithm based on exploiting modification direction, *Multimed. Tools. Appl.*, (2018), online. DOI: 10.1007/s10773-018-3716-4
27. F. Grosshans and P. Grangier, Continuous variable quantum cryptography using coherent states, *Phys. Rev. Lett.*, **88** (2002), 057902.
28. S. Olivares, M.G.A. Paris and R. Bonifacio, Teleportation improvement by inconclusive photon subtraction, *Phys. Rev. A*, **67** (2003), 032314.
29. J. N. Wu, S. Y. Liu, L. Y. Hu, et al., Improving entanglement of even entangled coherent states by a coherent superposition of photon subtraction and addition, *J. Opt. Soc. Am. B*, **32** (2015), 2299.
30. Y. Guo, W. Ye, H. Zhong, et al., Continuous-variable quantum key distribution with non-Gaussian quantum catalysis, *Phys. Rev. A*, **99** (2019), 032327.
31. L. P. Van and S. L. Braunstein, Multipartite entanglement for continuous variables: a quantum teleportation network, *Phys. Rev. Lett.*, **84** (2000), 3482–3485.
32. H. Ma, P. Huang and W. Bao, Continuous-variable quantum identity authentication based on quantum teleportation, *Quantum Inf. Process.*, **15** (2016), 2605–2620.
33. C. Berrou and A. Glavieux, Near optimum error correcting coding and decoding: turbo-codes, *IEEE T. Commun.*, **44** (1996), 1261–1271.
34. R. G. Gallager, Low-density parity-check codes, *IEEE Commun. Surv. Tut.*, **13** (2011), 3–26.
35. T. C. Ralph, Continuous variable quantum cryptography, *Phys. Rev. A*, **61** (1999), 010303.
36. W. P. Bowen, N. Treps, B. C. Buchler, et al., Experimental investigation of continuous-variable quantum teleportation, *Phys. Rev. A*, **67** (2003), 032302.
37. J. Z. Huang, C. Weedbrook, Z. Q. Yin, et al., Quantum hacking on continuous-variable quantum key distribution system using a wavelength attack, *Phys. Rev. A*, **87** (2013), 062329.