Two-step unsymmetrical quantum key distribution protocol using GHZ triplet states

HUANG Peng¹ (✉), LIU Ye¹, ZHOU Nan-run¹, ZENG Gui-hua²

¹. Department of Electronic Information Engineering, Nanchang University, Nanchang 330031, China
². State Key Laboratory of Advanced Optical Communication Systems and Networks,
   Department of Electronic Engineering, Shanghai Jiaotong University, Shanghai 200240, China

Abstract

The security, efficiency, transmission distance and error rate are important parameters of a quantum key distribution scheme. In this article, the former two parameters are focused on. To reach high efficiency, an unsymmetrical quantum key distribution scheme that employs Greenberger-Horne-Zeilinger (GHZ) triplet states and dense coding mechanism is proposed, in which a GHZ triplet state can be used to share two bits of classical information. The proposed scheme can be employed in a noisy or losy quantum channel. In addition, a general approach to security analysis against general individual attacks is presented.

Keywords two-step, unsymmetrical quantum key distribution, GHZ triplet states

1 Introduction

Since Bennett and Brassard presented the pioneer quantum key distribution (QKD) scheme in 1984, known as BB84 protocol [1], much attention has been paid to the QKD protocol. This protocol has been developed in principle and application of quantum secret key. Many QKD schemes have been proposed, which can be divided into two types, i.e., nondeterministic and deterministic schemes. These two types have different characteristics. For nondeterministic schemes, the sender (Alice) chooses randomly two sets of measuring bases (there are at least two sets of nonorthogonal bases) to create two kinds of orthogonal states and transmits them to the receiver (Bob), then Bob also chooses randomly one of the two sets of bases to measure the received states. There is only a certain probability that Alice and Bob choose the same bases. Thus Alice cannot determine which bit values Bob can receive before they exchange classical information. Typical schemes of this type are BB84 protocol [1], B92 protocol [2], Einstein-Podolsky-Rosen (EPR) protocol [3] and the newly proposed QKD protocol in Ref. [4]. To obtain the final secret key, Alice and Bob drop the qubits whose measurements bases are not uniform, and then use several classical treatments such as error correction [5], privacy amplification [6] to reduce the error rate and improve the security. The nondeterministic protocol is unfavorable because of its low efficiency (mostly less than 50%) and high cost. By contrast, as for the deterministic schemes, Alice and Bob choose the same orthogonal measurement bases. Thus, they can get the same results deterministically; otherwise the quantum channel is disturbed. Typical protocols of this kind are the ones presented in Refs. [7–12].

The so-called ping-pong protocol is a typical deterministic QKD scheme [10]. It has been proven efficient because it can be used to transmit quantum states in a deterministic way. Although it was also proven insecure for transmitting secret message in a noisy quantum channel [13], it is still secure for QKD. Several ping-pong protocols have been proposed [14–17]. However, high losses in these ping-pong schemes are caused by the application of the two-way channel. To achieve higher efficiency with lower cost, an unsymmetric QKD protocol using GHZ triplet entanglement states was proposed in Ref. [18], where the unsymmetrical characteristic avoids the waste of qubits arising from bases reconciliation and can achieve high application efficiency. Based on dense coding and GHZ states, Ref. [19] proposed a quantum secure direct communication (QSDC) scheme based on EPR state, in which the two-step transmission of EPR states makes the whole communication secure. However, these QKD schemes still
feature low efficiency and insufficient security proof.

In this article, the authors put forward a novel unsymmetrical QKD protocol where the information particles are sent by two steps. By exploiting the dense coding and GHZ triplet states, a GHZ state can be used to obtain two bits of classical secret key, which results in high application efficiency. In addition, they present strong proof for security analysis for the proposed scheme against general individual attacks. The article is organized as follows: in Sect. 2, a two-step unsymmetrical QKD scheme is proposed. Sect. 3 shows the analysis of its efficiency. In Sect. 4, detailed security proofs are studied under two typical eavesdropping attack strategies, i.e., the intercept-and-resend attack strategy and the entanglement-and-measure attack strategy. The information theoretic analysis is presented against the entanglement-and-measure attack strategy. The application of the QKD scheme in imperfect quantum channel is depicted in Sect. 5. Finally, conclusions are drawn in Sect. 6.

2 The two-step unsymmetrical QKD protocol

The proposed protocol employs three-particle GHZ states and dense coding technique. Suppose the maximally entangled three-particle state is:

$$|\Phi^+_{\text{GHZ}}\rangle = \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)$$  \hspace{1cm} (1)

By employing the following eigenstates of Pauli operators $X$ and four Bell states [20]:

$$|x+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$
$$|x-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

$$|\phi^+\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$$
$$|\phi^-\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$$

The GHZ triplet state $|\Phi^+\rangle$ can be rewritten in terms of the base of $X$ of particle 1 and Bell states of particles 2 and 3 as follows:

$$|\Phi^+_{\text{GHZ}}\rangle = \frac{1}{\sqrt{2}}(|x+\rangle|\phi^+_2\rangle + |x-\rangle|\phi^-_2\rangle)$$  \hspace{1cm} (4)

If one performs a unitary operation $U_x = |0\rangle\langle 0| + |1\rangle\langle 1|$ or $U_z = \sigma_z = |1\rangle\langle 0| + |0\rangle\langle 1|$ on particle 3, the GHZ triplet state may be rewritten as:

$$|\Phi^+_{\text{GHZ}}\rangle = \frac{1}{\sqrt{2}}(|x+\rangle|\phi^+_2\rangle + |x-\rangle|\phi^-_2\rangle)$$

$$|\Phi^-_{\text{GHZ}}\rangle = \frac{1}{\sqrt{2}}(|x+\rangle|\phi^-_2\rangle + |x-\rangle|\phi^+_2\rangle)$$  \hspace{1cm} (5)

The above decompositions demonstrate correlations among three particles in the GHZ states. In Eq. (5), for example, if the first particle is in state $|x+\rangle$, then the Bell-basis measurement result of the other two particles must be in state $|\phi^+_2\rangle$ because of the correlation of the GHZ triplet state. According to Eqs. (5) and (6) and by the unitary operation, the correlation between the property of GHZ states and the unitary operations may be constructed in the following table.

Table 1 displays the correlation between the unitary operations and the states of GHZ particles. If only particle 1 is measured, the states of the other two particles are still not determined because of the unknown unitary operation. This characteristic can be used to design a QKD scheme. Suppose Alice and Bob pre-agree on that each of the four Bell bases can carry two qubits of classical information when encoding $|\phi^+\rangle$, $|\phi^-\rangle$, $|\phi^{0}\rangle$ and $|\phi^{1}\rangle$ as 00, 01, 10 and 11, respectively. The unsymmetrical QKD protocol using GHZ states is implemented in the following steps.

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Alice prepares a sequence of three-particle GHZ states and each particle is in the state $</td>
</tr>
<tr>
<td>2</td>
<td>$P_1$ is held by Alice as home particle-sequence. Alice sends $P_2$ particles to Bob. When Bob receives the particles, he randomly chooses a set of checking particles from $P_2$ and measures the chosen particles on the base $\sigma_z$, and then tells Alice the positions of the chosen particles and his measurement.</td>
</tr>
<tr>
<td>3</td>
<td>Alice randomly performs unitary operation $U_z$ or $U_x$ on the remaining $P_3$ particles (except the correlated particles with the $P_2$ checking particles which were measured in the above step). After operations, Alice transmits all the $P_3$ particles to Bob.</td>
</tr>
</tbody>
</table>
| 4    | Alice and Bob perform eavesdropping check:  
1) Bob chooses randomly one of the two sets of measurement basis (MB), i.e., $\sigma_z$ and $\sigma_x$ to measure the checking particles in $P_2$.  
2) Bob tells Alice which MB he has chosen for each photon and the measurement outcomes.  
3) Alice uses the same MB to measure the corresponding $P_1$ particles and then tells Alice which MB he has chosen for each photon. |

The two-step unsymmetrical QKD protocol using GHZ states is implemented in the following steps.

Table 1 The correlation results between the unitary operations and the GHZ triplet states

| State of particle 1 | $|x-\rangle$ | $|x+\rangle$ |
|---------------------|-------------|-------------|
| Unitary operation on particle 3 | $U_x$ | $U_1$ | $U_z$ | $U_1$ |
| State of particle 2, 3 | $|\phi^+\rangle$ | $|\phi^-\rangle$ | $|\phi^{0}\rangle$ | $|\phi^{1}\rangle$ |
checking particles.

4) Using the correlation of GHZ triplet state, Alice checks their measurement results. If no eavesdropping exists, their results should be in given correlations. Because after the measurement on $P_1$ checking particles in step 2, the $P_1$ checking particles that belong to Alice and the corresponding $P_1$ checking particles that belong to Bob have collapsed in Bell state $|\phi^+\rangle$ or $|\phi^-\rangle$, their results satisfy the following equation:

$$|\phi_b\rangle = \frac{1}{\sqrt{2}}\left(|\phi^+\rangle|x^+\rangle_x_2 + |\phi^-\rangle|x^-\rangle_x_2\right) =$$

$$\frac{1}{2}\left(|x^+\rangle|x^+\rangle_x_2|x^+\rangle_x_3 + |x^-\rangle|x^-\rangle_x_2|x^+\rangle_x_3 +$$

$$|x^+\rangle|x^+\rangle_x_2|x^-\rangle_x_3 - |x^-\rangle|x^-\rangle_x_2|x^-\rangle_x_3\right) =$$

$$\frac{1}{2}\left(|0\rangle_x_1|x^+\rangle_x_2 + |1\rangle_x_1|x^-\rangle_x_2 +$$

$$|0\rangle_x_1|x^-\rangle_x_2 - |1\rangle_x_1|x^+\rangle_x_2\right) \quad (7)$$

i.e., if Bob’s measurement result in step 2 is $|x^+\rangle$ or $|x^-\rangle$, then their measurement results in this step must be correlated with the Bell states $|\phi^+_1\rangle$ or $|\phi^-_1\rangle$. In fact, in this two-step transmission, Eve can only disturb the transmission and cannot steal the key information because she can only get a useless single state from a Bell state. If she intercepts the corresponding $P_2$ and $P_3$ particles to take Bell-basis measurement simultaneously, the errors must be induced. If the error rate is reasonably low, Alice and Bob can then entrust the process and continue. Otherwise, Alice and Bob abandon the communication and repeat the procedures from the beginning.

Step 5 Bob makes Bell-basis measurement on the remaining $P_2$ particles and the corresponding $P_1$ particles he has received (except the checking particles), then decodes the measurement results $|\phi^+_1\rangle$, $|\phi^-_1\rangle$, $|\phi^+_2\rangle$ and $|\phi^-_2\rangle$ as 00, 01, 10 and 11, respectively.

Step 6 After Bob completes his measurements, Alice measures the remaining home particles in basis $\sigma_x$ and decodes the outcomes $|x^+\rangle$ and $|x^-\rangle$ as 00 and 01, respectively. Alice asks Bob to tell him his measurement results in some random positions. According to her measurement outcomes and the performed unitary operations, Alice can conclude Bob’s measurement outcomes. Table 1 shows the detailed property of these correlations. If the error rate is larger than a bound, Eve’s attack is detected and the transmission is aborted.

Step 7 According to the above discussion, Alice judges Bob’s measurement results and make her results be consistent with Bob’s. For example, if Alice’s measurement result is $|x^+\rangle$, i.e. 00, and Bob’s measurement result is $|\phi^-\rangle$, i.e. 01, then Alice changes her result to 01.

Step 8 Alice and Bob use techniques such as data sifting, error correction, and privacy amplification to process the sharing secret key to secure the privacy of the key. Then the communication is successfully terminated.

The proposed protocol is unsymmetrical since Alice is distributed one particle sequence, $P_1$, and Bob is distributed two particle sequences, $P_2$ and $P_3$. As discussed above, Alice and Bob can ensure the security of the home sequence $P_1$, thus Eve’s eavesdropping strategy is located on $P_2$ particles and $P_3$ particles. The security proofs below will show that Eve will be found out if she eavesdrops the quantum line. It is of interest that Eve cannot read out information in Bell states even if she captures any one of the two transmission sequences, because no one can read the information from one particle state of a Bell state alone. In this way, no key information will be leaked to Eve, that is, the scheme is completely secure. Moreover, the capacity is high in this scheme, because each GHZ state can be used to carry two bits of classical information.

3 Application efficiency

As is known, QKD efficiency is an important issue that describes the utilization efficiency of the quantum states used in protocols. In the BB84 [1] and B92 [2] protocols, suppose the lost qubits is $l$, which is caused by imperfectness of the quantum channel, and consider the discarded qubits because of different measurement bases. To obtain $L$ qubits key, Alice has to send more than $2(L + l)$ qubits to Bob. Here, the authors propose a certain parameter as application efficiency denoted by the product of utilization efficiency of the quantum states and the capacity of quantum states, that is, the optimal application efficiency of the BB84 is $\eta_{BB84} = \frac{L}{2(L + l)} < 50\%$. As for the ping-pong protocol [10], because of the two-way channel, the waste of qubits arising from base reconciliation can be avoided, whereas the use of the two-way channel causes doubled loss because the communication distance is doubled. Hence, the application efficiency of the ping-pong protocols can be written as $\eta_{ping-pong} = \frac{L}{L + 2l}$.

In Ref. [18] a secure unsymmetrical quantum key distribution protocol is proposed, in which a GHZ triplet state can be used to obtain the secret key. Except the lost qubits resulting from imperfectness of physical devices, the unsymmetrical characteristic makes all the transmitted qubits useful and a GHZ state can be used to obtain one bit of classical secret key. Therefore, the application efficiency of
this protocol is \( \eta_{\text{sym}} = \frac{L}{L+L} < 100\% \). In the protocol proposed in this article, Alice sends two correlated sequences in a two-step way to obtain the secret key. By exploiting dense coding mechanism, one GHZ triplet state can be used to obtain two bits of classical information. The application efficiency of the protocol is:

\[
\eta_{\text{novel}} = \frac{2L}{L+2l} < 200\% \quad (8)
\]

As discussed above, one can see that for the same lost qubits \( l \), \( \eta_{\text{BB84}} < \eta_{\text{novel}} < \eta_{\text{sym}} \) can be found. That is, the proposed scheme achieves the highest application efficiency.

4 Security proofs

Eve has two typical possible strategies of eavesdropping, i.e., the intercept-and-resend attack and the entanglement-and-measure attack. In the following section, the failure of these attack strategies on obtaining the secret key information is described in detail.

4.1 The intercept-and-resend attack

The secret key is obtained using the divided three sequences of GHZ triplet states, where sequence \( P_1 \) are held by Alice as the home particles and the particles of sequence \( P_2 \) and \( P_3 \) are the transmission particles. Here, the home particles are retained safely in Alice’s station. Before eavesdropping check, Eve has no access to the home particles. Suppose Eve has managed to access Alice and Bob’s communication line. To get the secret key carried on the four Bell states, she first intercepts \( P_2 \) particles and sends on to Bob another particle, later she intercepts the correlated \( P_3 \) particle and sends on to Bob another particle, then she may conduct Bell-basis measurement to read out the secret key. In this case, Eve cannot obtain the secret key because the particles in Alice’s station and the particles in Bob’s station are not in a GHZ triplet state. There are no correlated or anti-correlated results. Thus Eve’s interception will introduce error and can be easily detected by Alice and Bob in step 4. Hence, the proposed protocol is secure against the attack of intercept-and-resend attack.

4.2 The two-step entanglement-and-measure attack

Suppose Eve is an evil quantum physicist able to build all devices within the laws of quantum mechanics. Eve has two kinds of entanglement-and-measure attack, i.e., she uses one ancilla or two ancillas to obtain the secret key. If she gives priority to obtain much more information instead of detection probability, she may employ the two ancillas entanglement attack, otherwise, the former method will be employed. Here, the most effective method of the entanglement-and-measure attacks is considered, i.e., using two ancillas to obtain the key information as follows.

To gain information, Eve first intercepts the transmission particles of sequence \( P_2 \) from Alice and performs the operation \( E_1 \) on both the transmission particles and the ancillary state \( \varepsilon \). After this operation, Eve sends the \( P_2 \) particles to Bob. When Bob receives the \( P_2 \) particles, he will perform the operations as usual since he does not know Eve’s operations. After Eve intercepts the \( P_3 \) particles from Alice, she performs another operation \( E_2 \) on the \( P_3 \) particles and the ancillary state \( \eta \). By employing the obtained results from \( \varepsilon \) and \( \eta \), Eve tries to achieve information from the secret key. However, not only no key information is disclosed to Eve, but also Alice and Bob can detect Eve’s disturbance. The whole procedure of this intercept-and-resend attack strategy is plotted in Fig. 1.

![Fig. 1 Eve’s intercept-and-resend attack strategy](image_url)
where $|\psi_w\rangle$, $|\theta \rangle$, $|\phi \rangle$, $|\eta \rangle$ and $|\eta_0\rangle$, $|\eta_1\rangle$, $|\eta_0\rangle$, $|\eta_i\rangle$ are pure states uniquely determined by the unitary operations $E_i$ and $E_2$, respectively. Unitary operation requires $|A_i\rangle^2 + |B_i\rangle^2 = 1$. Without loss of generality, it is assumed that $\langle \psi_{w0} | \psi_{w1} \rangle = \langle \theta | \phi \rangle = \langle \psi_{0i} | \psi_{1i} \rangle = 0$ and $\langle \psi_{w0} | \psi_{1i} \rangle = \cos \theta_+ \phi$, $\langle \psi_{0i} | \psi_{11} \rangle = \cos \phi$, where $\zeta = \epsilon$, $\eta$, and $\theta_+ \phi$, $\phi_\theta$, $\phi_\eta \in [0, \pi/2]$.

We divide the whole GHZ triplet sequence with the length of $n$ into two parts, i.e., the checking sequence with length of $c$ which is used for eavesdropping check in step 4 and the remaining sequence with length of $n-c$ which are used to obtain secret key, denoted as message sequence. Next, the mutual information $I(A, B)$ between Alice and Bob and the mutual information $I(B, E)$ between Bob and Eve is calculated according to this division.

Because of Eve’s disturbance, Bob will receive the perturbed states. The error probability can then be evaluated from the checking sequence at Bob’s station by squaring the coefficients of the states altered after Eve’s attack with Eqs. (9)–(11) and (12)–(14),

$$d_{s,b} = \frac{P_s P_f + P_s P_f + B_s^2}{2}$$

(15)

where $P_s = \left[2|A_i\rangle^2 \left(1 + \cos \theta_\eta \phi \right) \right]^{-1} + \left[2|B_i\rangle^2 \left(1 + \cos \phi \right) \right]^{-1}$ for $\zeta = \epsilon$, $\eta$.

After Alice’s unitary operations $U_0$ and $U_1$ in step 3 and Eve’s entanglement operations $E_{\epsilon}$ and $E_2$, the two states of the system $|\phi\rangle_{\text{Giz}}$, and $|\phi\rangle_{\text{Giz}}$, of the message particle states can be described as:

$$|\Psi_i\rangle = E_i \left[E_i \left(|\phi\rangle_{\text{Giz}}, \otimes \psi\rangle \right) \right]$$

(16)

$$|\Psi_i\rangle = E_i \left[E_i \left(|\phi\rangle_{\text{Giz}}, \otimes \psi\rangle \right) \right]$$

(17)

With the tool of the Schmidt decomposition [20], the composite system states $|\Psi_i\rangle (i=1,2)$ are rewritten as

$$|\Psi_i\rangle = |x\rangle_1 \left(\lambda_1^i |\phi_1\rangle_{\phi_2} + \lambda_2^i |\phi_1\rangle_{\phi_2} + \lambda_3^i |\phi_1\rangle_{\phi_2} + \lambda_4^i |\phi_1\rangle_{\phi_2}\right) +$$

$$|x\rangle_2 \left(\lambda_1^i |\phi_1\rangle_{\phi_2} + \lambda_2^i |\phi_1\rangle_{\phi_2} + \lambda_3^i |\phi_1\rangle_{\phi_2} + \lambda_4^i |\phi_1\rangle_{\phi_2}\right)$$

(18)

where $\lambda_j (j=1,2,3,4)$ are Schmidt coefficients that satisfy

$$\sum_j (\lambda_j^i)^2 = 1$$

for $i=1,2$. Similarly, Eve will be detected if the states of the two transmission particles are not in the initial Bell states. The error probability for the message sequence can be calculated at Bob's station with Eq. (18),

$$d_{s,b} = \sum_{j=1}^{2} \sum_{j=1}^{2} (\lambda_j^i)^2$$

(19)

The error probability at Bob’s station equals to the probability of detecting Eve’s presence in the two eavesdropping check steps, hence the probability of Eve to be detected can be expressed as

$$P_e = 1 - (1 - d_{s,b}) (1 - d_{s,b})$$

(20)

Eve’s purpose is to acquire maximum information with minimum probability of being detected, thus she will make $P_e$ as low as possible. Without loss of generality, denote $d$ as the minimal detection probability, one can obtain that $P_e$ reaches the minimum value

$$d = (P_e)_{\text{min}} = \frac{1 - \cos \theta_\eta \cos \phi_\eta}{4}$$

(21)

under the conditions $|A_i\rangle = |A_i\rangle = 1$, $|B_i\rangle = |B_i\rangle = 0$. Correspondingly, $d_{s,b}$ and $d_{s,b}$ reach the minimum value ($d_{s,b} = (1 - \cos \theta_\eta \cos \phi_\eta)/4$ and $d_{s,b} = 0$, respectively. Although Eve’s operation is not the most general one, she can perform it on the whole procedure, and thus resulting in general consequence. The obtained maximum value of $d$ is 1/4 when $\cos \theta_\eta = 0$ or $\cos \phi_\eta = 0$. Considering the minimum detection probability in EPR protocol and that in Ref. [18], and supposing Eve uses the same entanglement-and-measurement attack operation, one can obtain the minimum detection probability as follows

$$d' = \frac{1 - \cos \theta}{4}$$

(22)

By comparing Eq. (21) with Eq. (22), $d > d'$ can be obtained, which means that the probability of detecting Eve’s eavesdropping in the proposed protocol is larger than that of the EPR protocol and the proposed protocol in Ref. [18], that is, Eve can be easily detected in the proposed protocol.

According to the Shannon information theory [21], the mutual information on the secret key between Alice and Bob can be derived as

$$I(A,B) = h(A) + h(B) - h(A,B)$$

(23)

where $h(A)$, $h(B)$ are the binary entropy at Alice and Bob’s stations, respectively, and $h(A,B)$ is the joint entropy
between Alice and Bob’s stations. The following can then be obtained:

$$I(A, B) = 2 + \sum_{a,b} P(A,B) \log_2 P(B \mid A) \tag{24}$$

where $a$ is the two-bit key message that Alice encodes and will share with Bob, and $b$ is the two-bit key message that Bob decodes from the Bell-basis measurement outcomes of Alice’s transmission of $P_2$ and $P_3$ particles, i.e., $a, b \in \{00, 01, 10, 11\}$. Since $P(A,B) = P(A)P(B \mid A)$, to obtain $I(A,B)$, it only needs to calculate $P(A)$ and $P(B \mid A)$. Obviously, $P(A) = 1/4$. Next, the authors show how to calculate the conditional probability $P(B \mid A)$. Take the following case as an example. First, calculate $P(00 \mid 00)$, i.e., the probability of Bob’s measurement outcome states being $|\phi^+\rangle$ when Alice’s encoded state on particles 2 and 3 is $|\phi^+\rangle$. Under the condition with the minimal detection probability, which corresponds to a special attack strategy, Eq. (16) can be simplified as

$$|\Psi_\varepsilon\eta\rangle = \frac{1}{\sqrt{2}} \left[ x^+ \right] (|\varepsilon\eta\rangle_{H_0} + |\varepsilon\eta\rangle_{H_1}) |\phi^+\rangle + (|\varepsilon\eta\rangle_{H_0} - |\varepsilon\eta\rangle_{H_1}) |\phi^-\rangle$$

Comparing with Eq. (5), one can find that $P(00 \mid 00) = 1/2(1 + \cos \theta_x \cos \theta_y)$. Similarly, the other conditional probability can be calculated in Eve’s special strategy. Therefore, Eq. (24) can be rewritten as

$$I(A, B) = 2 - \frac{1 + \cos \theta_x \cos \theta_y}{2} \tag{25}$$

The presence of the two parameters $(\theta_x, \theta_y)$ in Eqs. (21) and (26) makes it impossible to express the mutual information $I(A,B)$ as the function of the detection probability $d$ only. However, a lemma in Ref. [17] helps to correlate them so that Eve’s optimal incoherent attack consists in a balanced one for which $\theta_x = \theta_y$. Rewrite Eqs. (21) and (26) as

$$d = 1 - \left( \cos \theta_y \right)^2 \frac{1}{4} \tag{27}$$

The mutual information $I(A,B)$ is plotted as function of the detection probability $d$ in Fig. 2. It can be noted that the minimum mutual information $I(A,B)$ is 1 bit when $d = 0.25$. To acquire information, Eve must measure her ancillary states to obtain information about the secret key. The probability of distinguishing correctly between two states with scalar product $\cos \theta = (1 + \sin \theta)/2$. That is, for these two states Eve has $(1 + \sin \theta)/2$ probability of being unable to correctly distinguish them [22]. Suppose that Alice’s encoded key is 00. After Eve’s optimal strategy, the ancillary states at Eve’s station is $|\varepsilon\eta\rangle_{H_0} + |\varepsilon\eta\rangle_{H_1}$ or $|\varepsilon\eta\rangle_{H_0} - |\varepsilon\eta\rangle_{H_1}$. The mutual information between Bob and Eve with Eve’s optimal strategy can be expressed as

$$I(B, E) = 2 + \sum_\varepsilon P(B \mid E) 1bP(E \mid B) = 2 + 1b \frac{1}{2} = 1 \tag{29}$$

It is shown in Fig. 2 that Eve’s maximal information on the secret key is 1 bit while the minimum information between Alice and Bob is also 1 bit. For a secure QKD scheme, the mutual information between Alice and Bob must be greater than that between Bob and Eve, i.e., $I(A,B)$ must be greater than $I(B, E)$. In the proposed scheme, $I(A,B)$ is constantly greater than $I(B, E)$ in the legitimate range $0 < d < 0.25$. Hence, the secret information rate in the scheme can be written as

$$\Delta I = I(A,B) - I(B, E) > 0 \tag{30}$$

Therefore, Alice and Bob can safely obtain a sequence of secret key by using the error correction and privacy amplification. When $\Delta I = 0 \, , \,$ i.e., the mutual information between Alice and Bob is equal to the mutual information between Bob and Eve, Eve’s presence can be detected by the eavesdropping check procedures in step 4 by setting corresponding bounds in the protocol. From the above security calculations, when the error rate is larger than the approximate bound 0.25, Eve’s intervention can be detected. Hence, the proposed scheme is secure under the two-step entanglement-and-measurement attack.
The two-step unsymmetrical QKD protocol in imperfect channel

In Sect. 2, an unsymmetrical QKD protocol in an ideal quantum channel was proposed, and its security was analyzed in Sect. 4. However, the practical application of the quantum channel is imperfect. In this section, the influence of imperfectness is studied on the proposed unsymmetrical QKD protocol. In Ref. [23] two kinds of imperfect quantum channel are studied, the noisy channel without loss and the lossy channel without noise. In this section, the presented scheme used in these two kinds of quantum channel is studied.

The proposed unsymmetrical QKD protocol is available in the noisy quantum channel. When in a noisy quantum channel, the noise will change the transmitted qubits and cause errors in the scheme. However, the quantum error correction codes [5] can provide an approach to preventing the errors. Thus with the application of the quantum error correction code, the proposed scheme is still available in the noisy quantum channel. Especially, the scheme is also available with revisions without the assistance of the quantum error correction code. First, the authors add the process of quantum privacy amplification [24] in step 4 and step 6 to filter the disturbed GHZ triplet states. Second, they change the error check bound. Since the error rate bound in step 4 and step 6 in the ideal quantum is 0.25 and 0, thus the error rate bound has to be set as $R_1 = \alpha + 0.25$ and $R_2 = \alpha$. These are the thresholds to judge Eve’s existence. When the error rate is beyond any of the bounds, Eve exists; otherwise, Eve does not exist. The modified scheme is also secure under the two kinds of the attack strategy discussed in Sect. 4. The analysis in Sect. 4 is suitable for the intercept-and-resend attack after the process. If Eve adopts the second kind of attack strategy, Eve cannot obtain any key information, either. Because the technique of the quantum privacy amplification is actually working as the entanglement purification, the privacy amplification process with sequences of $P_2$ and $P_3$ makes the distributed GHZ triplet states in their maximal entanglement, which makes Eve’s entanglement-and-measurement attack effortless.

When the imperfect quantum channel is lossy, and the lossy coefficient of the employed quantum channel is $\beta$, Bob will receive $(1-\beta)n$ particles of sequences $P_2$ and $P_3$, respectively. A wise eavesdropper will replace the lossy channel with an ideal one and obtain the other $\beta n$ particles of each sequence $P_2$ and $P_3$ without detection by Alice and Bob. Using this method, Eve may obtain information about the secret key. However, the leakage of the key information can be avoided by a simple modification in the proposed protocol. First, denote the loss particles obtained by Eve in step 2 and step 3 as $G_1 = \{P_1^0, P_1^1, ..., P_1^n\}$ and $G_2 = \{P_2^0, P_2^1, ..., P_2^n\}$, respectively, where $P_i^j (i = 2, 3; j = 1, 2, ..., \beta n)$ denotes particles. Second, after Alice sends particles of sequence $P_2$ in step 2 and sequence $P_3$ in step 3, Alice and Bob discard the GHZ triplet states correlated to $G_1$ and $G_2$. Hence, the leakage particles caught by Eve are useless according to the scheme, and the modified scheme is still available and secure in the lossy quantum channel. In the modified protocol, the discarded particles in $G_1$ and $G_2$ may be in the same GHZ states. Therefore, if Alice and Bob need to obtain $2n$ bits secret key, Alice should prepare $n/(1-2\beta)$ qubits of GHZ triplet states.

Conclusions

A two-step unsymmetrical quantum key distribution protocol of high efficiency is proposed, in which GHZ triplet states are used to obtain the secret key. By exploiting the dense coding mechanism, a GHZ triplet state can be used to obtain two bits of classical secret key. Compared with the ping-pong scheme and the proposed QKD protocol in Ref. [18], the proposed scheme has a high capacity and can achieve higher efficiency with lower cost. This article also considers Eve’s two kinds of typical general individual attack strategies, i.e., the intercept-and-resend attack and the two-step entanglement-and-measurement attack. A general approach to security analysis is also presented in information theory against Eve’s optimal entanglement-and-measurement attack strategy. The detailed proofs show that the proposed protocol is available and secure.

Acknowledgements

This work was supported by the National Natural Science Foundation of China (60773085, 10647133), the Natural Science Foundation of Jiangxi Province(2007GQS1906), the Research Foundation of the Education Department of Jiangxi Province ([2007]22), the Key Project in the 11th Five-Year Plan on Education Science of Jiangxi Province (07ZD017), the Innovation Project of Jiangxi Graduate Education(YC07A033), and the Scientific Research Starting Foundation for the Recruit Talent of Nanchang University of China.

References


(Editors: ZHANG Ying)

From p. 113


(Editor: WANG Xu-ying)