Using Decoy-States Quantum Secure Communication Protocol Based on Entangled W State Over Collective-Noise Channels

Xiaotian Liu [1, a], Dandan He [2, b]

[1]School of Information Engineering, Shanghai Maritime University, Shanghai 200120, China;

[2]Department of Information, Beijing University of Technology, Beijing 100020, China;

[a]chansulli@163.com, [b]1543151736@qq.com

Abstract

At present, the entangled W state has strong anti-decoherence, which can better prevent quantum scattering, and is often used in quantum communication. Aiming at the transmission of entangled W state in the channel, this paper presents a protocol that can resist the impact of combined phase-only unitary noise and joint rotational unitary noise on information transmission. By using the honeypot thought and using the four-particle cluster state as the decoy particle randomly inserted in the sending sequence and performing threshold analysis, it can be determined whether the adversary eavesdropped on the information. The adversary can not only obtain 25% of the secret key, and each quantum bit interception Detection efficiency can reach 43.8%. Through the analysis of the information entropy security, it can be proved that this protocol can resist many kinds of attack such as internal attack such as participant attack, external attack such as double C-NOT attack, entanglement measurement attack and Trojan horse attack. In addition, this protocol can reach higher Quantum Bit Efficiency and Information Efficiency.

Keywords

Entangled W state; decoy particle; participant attack; C-NOT attack; eavesdropping detection.

1. Introduction

Quantum cryptography is an interdisciplinary subject of quantum mechanics, quantum optics and classical cryptography. Due to the characteristics of quantum entanglement, quantum communication can guarantee the absolute security of communication data. High-order quantum entangled states are currently widely used. Application[1][2][3][4]. At present, Verstraete, Dehaene et al. believe that the four-particle entangled state is divided into nine categories [5], such as the W state, the cluster state, the W state and so on.

In order to prepare a quantum state remotely, an entangled quantum system is needed. At present, the preparation of the entangled W state is a relatively mature technology, which can better prevent quantum de-dispersion, has strong anti-decoherence. It can delay the occurrence of collapse caused by the interaction of quantum systems and the environment [6]. Since the physical system is a real environment, the interaction between the state and the environment in the physical system changes when interacting with the external environment, so that the coherence of the state in the quantum system is attenuated. For example, noise in the environment will affect the maintenance of quantum coherent states.

In 1984, Bennett and Brassard proposed a quantum key distribution scheme, later called the BB84 protocol [7], which formed a different polarization state for the quantum states $|0\rangle$ and $|1\rangle$ randomly generated by Alice according to the choice of the preparation basis. This proved to be an absolutely secure communication protocol. In 2005, Wang proposed a quantum key distribution scheme to overcome joint noise [8], which does not need any collective quantum measurement or quantum memory.

In 2008, Li et al. [9] used two Bell states that can overcome channel noise to encode one-bit key information, two sets of non-orthogonal basis vectors are constructed by changing the order of photons to ensure the security of the key distribution process and to resist joint dephasing noise. This protocol introduces the idea into the information transmission of the entangled W state in the channel, which can well resist the influence of joint noise. Moreover, Gao et al. [10] proposes that in the CQSDC protocol based on the GHZ state, under the C-NOT attack, the receiver can illegally obtain 33.3% of the secret key information without authorization by the controller.

In [11], the honeypot scheme was used in the protocol, and the three-particle GHZ state was used as a honeypot particle to detect channel safety. This paper introduces this idea into the four-particle entangled state communication, using the four-particle cluster state as the decoy state, which means that the communication party only needs to detect the decoy particles to know whether it is attacked by Eve, effectively preventing multiple attacks. Means greatly enhance the safety and quality of communication.

2. Basic theory

What QKD does is also the secure distribution of classic keys, which are considered classic systems for information security. The most commonly used quantum state is a set of 2^n orthogonal normalized bases in a two-dimensional Hilbert space: $|0\rangle$， $|1\rangle, \ldots, |2^n - 1\rangle$. The maximum entangled state of the n-particles is prepared by the parametric down-conversion method in this space:

$$|\Phi\rangle_{ab}=\sum_{i=0}^{2^n-1} \alpha^i \tag{1}$$

And according to the decoherence of the quantum state:

$$\sum_{i=0}^{2^n-1}|\alpha^i|=1 \tag{2}$$

The coefficient α^i is used to carry the data to measure the quantum state and collapse to the state $|i\rangle$ with the probability of $|\alpha^i|^2$. By transmitting these quantum states, information can be transmitted. In this protocol, the entangled W state is used to transfer the secret key, and the four-particle cluster state is used as the decoy state of the honeypot.

2.1 Non-cloning theorem of quantum states

Quantum entanglement is an attribute of the association between subsystems or degrees within a quantum system. The superposition of the probability amplitudes shows a unique interference phenomenon between the quantum, and such a quantum superposition state is called an entangled state. If a single measurement of an entangled state does not yield all the information of a quantum state, multiple measurements must be made.

For example, copy the entangled state $|\Psi\rangle\otimes|\Phi\rangle$ to $|0_{A/B}\rangle$:

$$|\Psi\rangle\otimes|\Phi\rangle \xrightarrow{U} |0\rangle \tag{3}$$

Process the results:

$$|\omega\rangle\otimes|0\rangle \xrightarrow{U} |\omega\rangle\otimes|\omega'\rangle = (|\Psi\rangle + |\Phi\rangle)\otimes|0\rangle=|\Psi_A\rangle\otimes|\Psi_B\rangle + |\Phi_A\rangle \tag{4}$$

However, the results of this formula do not correspond to the actual results, according to the principle of linear superposition:

$$|\omega\rangle\otimes|\omega'\rangle = |\Psi_A\rangle\otimes|\Psi_B\rangle+|\Psi_A\rangle\otimes|\Phi_B\rangle + |\Phi_A\rangle\otimes|\Psi_B\rangle + |\Phi_A\rangle\otimes|\Phi_B\rangle \tag{5}$$

So we can judge that quantum is not able to obtain information by copying a large number of samples. We can generalize to a function $f(X_i)$, where $f(X_i)$ and X_i are used as the quantum states of the

stored information, which can form a more complex entangled state containing the overall information of the function:

$$\sum_{i=1}^{n}|X_i\rangle\otimes|f(X_i)\rangle = |X_1\rangle\otimes|f(X_1)\rangle + |X_2\rangle\otimes|f(X_2)\rangle + \cdots + |X_n\rangle\otimes|f(X_n)\rangle \quad (6)$$

3. Quantum key agreement protocol

3.1 In the case of collective phase-out noise

The combined de-phase noise on the quantum channel produces a phase difference between the horizontally polarized state and the vertically-polarized state of the polarized photon, and the quantum state of the system undergoes a collective phase-off error.

Among them, the collective phase-out noise matrix operator is:

$$U_{dp}=\begin{pmatrix} V & H \\ V & e^{i\varphi} \end{pmatrix} \quad (7)$$

The quantum state of the system has a collective phase reversal error, and the effect on the logical bits can be expressed as follows:

$$U_{dp}|H\rangle \xrightarrow{U} |H\rangle \quad (8a)$$

$$U_{dp}|V\rangle \xrightarrow{U} e^{i\varphi}|V\rangle \quad (8b)$$

$$U_{dp}|+\rangle \xrightarrow{U} 1/\sqrt{2}(|H\rangle_{dp}+|V\rangle_{dp})=e^{i\varphi}|V\rangle+|H\rangle \quad (8c)$$

$$U_{dp}|-\rangle \xrightarrow{U} 1/\sqrt{2}(|H\rangle_{dp}-|V\rangle_{dp})=-e^{i\varphi}|V\rangle+|H\rangle \quad (8d)$$

The qubits $|H\rangle_{dp}=|HV\rangle$ and $|V\rangle_{dp}=|VH\rangle$, and their arbitrary superposition states, are resistant to the effects of noise on the quantum system. After the two parties start communication, set the quantum state coding method negotiated between Alice and Bob as:

If in Alice's measurement result, the results are the same, then the code 1 is obtained, otherwise it is 0; If in Bob's measurement result, the results are the same, then the code 0 is obtained, otherwise it is 1;

Table 1 Each collapse state and the corresponding information

Observer	$\|HH\rangle$	$\|HV\rangle$	$\|VH\rangle$	$\|VV\rangle$
Alice	1	0	0	1
Bob	0	1	1	0

The protocol are as follows:

First, Alice prepares n four-particle polarization entangled W states .

$$|W_{dp}\rangle_{ABCD}=1/2\,(|VH\rangle|H\rangle_{dp}|H\rangle_{dp}+|HV\rangle|H\rangle_{dp}|H\rangle_{dp}+|HH\rangle|V\rangle_{dp}|H\rangle_{dp}|HH\rangle|H\rangle_{dp}|V\rangle_{dp})_{ABCD}$$

$$= 1/2\,(|VH\rangle_{AB}|HV\rangle_{C1C2}|HV\rangle_{D1D2} + |HV\rangle_{AB}|HV\rangle_{C1C2}|HV\rangle_{D1D2} + |HH\rangle_{AB}|VH\rangle_{C1C2}|HV\rangle_{D1D2}+|HH\rangle_{AB}|HV\rangle_{C1C2}|VH\rangle_{D1D2}) \quad (9)$$

Four-particle cluster state $|\rho\rangle$ as a decoy state:

$$|\rho_{dp}\rangle_{ABCD}=1/2\,(|VHHH\rangle+|HHVV\rangle+|VVHH\rangle+|VVVV\rangle)_{ABCD} \quad (10)$$

Then Alice randomly selects a sufficient number of decoy particles m and randomly inserts the sequence S_B consisting of particles CD, S_B ={ { $C_1D_1(1)$， $C_2D_2(1)$}， {$C_1D_1(2)$， $C_2D_2(2)$ }， …， { C_1D_1 (n)， C_2D_2 (n) } }. Alice then retains the sequence S_A of the composition of the particles AB, and sends the sequence S_B to Bob over a secure quantum channel, S_A={ A_1B_1， A_2B_2， …， A_nB_n}.

When Bob receives the sequence S_B and communicates with Alice through the classic channel, Alice tells Bob to deceive the position of the bit. Bob performs a $Z \otimes Z$ measurement on the decoyed particle, and then informs Alice of the measurement. Alice uses this result to deceive the quantum initial state. Perform comparison and observe the state change, calculate the error rate according to the measurement result and judge whether the error rate exceeds the threshold. If it is lower than the threshold, it means that it is not attacked by the enemy Eve. Otherwise, it is determined that the key is eavesdropped by Eve, and the protocol key needs to be discarded.

After removing the decoy particles, Bob performs two C-NOT operations on C_1C_2 and D_1D_2 in sequence S_B, respectively, where particle C_1C_2 is used as the control qubit and particle D_1D_2 is the target qubit: $|C_1\rangle|C_2\rangle \rightarrow |C_1\rangle|C_2 \oplus C_2\rangle$, $|D_1\rangle|D_2\rangle \rightarrow |D_1\rangle|D_2 \oplus D_2\rangle$.

After this operation, the quantum entangled W state system will become another new quantum state $|W'\rangle$:

$$\begin{aligned}|W_{dp}\rangle_{ABCD} &= 1/2(|VH\rangle_{AB}|HV\rangle_{C1C2}|HV\rangle_{D1D2} + |HV\rangle_{AB}|HV\rangle_{C1C2}|HV\rangle_{D1D2}|HH\rangle_{AB}|VV\rangle_{C1C2}|HV\rangle_{D1D2} \\ &\quad + |HH\rangle_{AB}|VV\rangle_{C1C2}|HV\rangle_{D1D2}) \\ &= 1/2\,(|VHHH\rangle + |HVHH\rangle + |HHVH\rangle + |HHHV\rangle)_{ABC1D1}|VV\rangle_{C2D2} \end{aligned} \tag{11}$$

Then Alice performs $Z \otimes Z$ measurement on the numbered particles corresponding to the sequence S_A, and Bob also performs $Z \otimes Z$ measurement on the sequence S_B particles. According to the characteristics of the entangled quantum state and the encoding method previously agreed by Alice and Bob, both parties can obtain the same key accordingly.

3.2 In the case of collective rotating noise

The combined rotating noise on the quantum channel causes the polarized photons to rotate. This phenomenon occurs at both the transmitting end and the receiving end, causing noise errors in the quantum state of the system.

Among them, the collective rotating noise matrix operator can be expressed as:

$$U_{rot} = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix} \tag{12}$$

In the formula, the collective reversal rotation noise parameter is φ, and the parameter φ changes with time. The influence of noise on logical bit $|H\rangle$ and $|V\rangle$ can be expressed as:

$$\begin{aligned} U_{rot}|H\rangle &\xrightarrow{U} \sin\theta|H\rangle + \cos\theta|V\rangle \\ U_{rot}|V\rangle &\xrightarrow{U} -\sin\theta|H\rangle + \cos\theta|V\rangle \end{aligned} \tag{13}$$

Their superposition state can be expressed as:

$$\begin{aligned} |+\rangle_{rot} \xrightarrow{U} 1/\sqrt{2}(|H\rangle_{rot} + |V\rangle_{rot}) &= 1/\sqrt{2}\,(-\sin\theta|H\rangle + \cos\theta|V\rangle + \cos\theta|H\rangle + \sin\theta|V\rangle) \\ &= 1/\sqrt{2}\,[(\cos\theta - \sin\theta)|H\rangle + (\cos\theta - \sin\theta|V\rangle] \end{aligned} \tag{14}$$

$$|-\rangle_{rot} \xrightarrow{U} 1/\sqrt{2}(|H\rangle_{rot} - |V\rangle_{rot}) = 1/\sqrt{2}\,(\sin\theta|H\rangle - \cos\theta|V\rangle + \cos\theta|H\rangle + \sin\theta|V\rangle)$$

$$= 1/\sqrt{2}[(\sin\theta + \cos\theta)|H\rangle + (\sin\theta - \cos\theta)|V\rangle] \quad (15)$$

The affected logical bits are marked as:

$$|H\rangle_{\text{rot}} = |\phi^+\rangle|V\rangle_{\text{rot}} = |\psi^-\rangle \quad (16)$$

The superposition state can be expressed as follows:

$$|+\rangle_{rot} \xrightarrow{U_{\text{rot}}} 1/\sqrt{2}(|H\rangle_{rot} + |V\rangle_{rot}) = 1/\sqrt{2}(|\phi^+\rangle + |\psi^-\rangle)$$

$$|-\rangle_{rot} \xrightarrow{U_{\text{rot}}} 1/\sqrt{2}(|H\rangle_{rot} - |V\rangle_{rot}) = 1/\sqrt{2}(|\phi^+\rangle - |\psi^-\rangle) \quad (17)$$

The logical bits $|H\rangle$, $|V\rangle$ and their superposition state are not affected by noise.

After the two parties start communication, set the quantum state code negotiated between Alice and Bob as:

If in Alice's measurement result, the high and low results are the same, then the code 1 is obtained, otherwise it is 0;

If in Bob's measurement result, the high and low results are the same, then the code 0 is obtained, otherwise it is 1;

Table 2 Each collapse state and the corresponding information

Observer	$\|HH\rangle$	$\|HV\rangle/\|VH\rangle$	$\|\phi^+\rangle\|\phi^+\rangle$	$\|\phi^+\rangle\|\psi^-\rangle/\|\psi^-\rangle\|\phi^+\rangle$
Alice	1	0	0	1
Bob	0	1	1	0

The protocol steps are as follows:

Alice is ready for n polarization entangled W states $|W_{rot}\rangle$:

$$|W_{rot}\rangle_{ABCD} = 1/2\,(|VHHH\rangle + |HVHH\rangle + |HHVH\rangle + |HHHV\rangle)_{ABCD}$$
$$= 1/2\,(|VH\rangle_{AB}|\phi^+\rangle_{C1C2}|\phi^+\rangle_{D1D2} + |HV\rangle_{AB}|\phi^+\rangle_{C1C2}|\phi^+\rangle_{D1D2}$$
$$+ |HH\rangle_{AB}|\phi^+\rangle_{C1C2}|\psi^-\rangle_{D1D2} + |HH\rangle_{AB}|\psi^-\rangle_{C1C2}|\phi^+\rangle_{D1D2}) \quad (18)$$

$$|\rho_{rot}\rangle_{ABCD} = 1/2(|\text{VH}\rangle_{\text{AB}}|HV\rangle_{C1C2}|HV\rangle_{D1D2} + |HV\rangle_{AB}|HV\rangle_{C1C2}|HV\rangle_{D1D2} +$$
$$|HH\rangle_{AB}|VV\rangle_{C1C2}|HV\rangle_{D1D2} + |HH\rangle_{AB}|VV\rangle_{C1C2}|HV\rangle_{D1D2})$$
$$= 1/2\,(|VHHH\rangle + |HVHH\rangle + |HHVH\rangle + |HHHV\rangle)_{ABC1D1}|VV\rangle_{C2D2} \quad (19)$$

With a four-particle cluster state as a decoy state$|\rho\rangle$:

$$|\rho_{rot}\rangle_{ABCD} = 1/2\,(|VHHH\rangle + |HHVV\rangle + |VVHH\rangle + |VVVV\rangle)_{ABCD} \quad (20)$$

Alice randomly selects a sufficient number of decoy bit m, a sequence of randomly inserted particle S_B'={{C_1'D_1' (1), C_2'D_2' (1)}, {C_1'D_1' (2), C_2'D_2' (2)}, …, {C_1'D_1' (n), C_2'D_2' (n)}}. Then

Alice retains the sequence S_A'=$\{A_1'B_1'$, $A_2'B_2'$, …, $A_n'B_n'\}$ composed of the particles AB, and transmits the sequence S_B' to Bob.

2) When Bob receives the sequence S_B and communicates with Alice through the classic channel, Alice tells Bob to deceive the position of the bit, Bob performs $Z \otimes Z$ measurement on the decoyed particle, and then informs Alice of the measurement result, Alice compare the decoy quantum with initial state. The error rate is calculated according to the measurement result and it is judged whether the error rate exceeds the threshold. If it is lower than the threshold, it is not attacked by Eve. Otherwise, it is determined that the key is eavesdropped by Eve, and the key needs to be discarded.

3) Alice then performs a $Z \otimes Z$ measurement on the numbered particles corresponding to the sequence S_A, and Bob performs a Bell measurement on the sequence S_B particles. According to the characteristics of the entangled quantum state and the encoding method previously agreed by Alice and Bob, both parties can obtain the same key accordingly.

4. Security analysis

4.1 Participant attack

If Alice is a non-honest sender, he wants to control the result of the transmitted string S_B, so that Bob cannot get the correctly encoded data, but in Protocol 3.1 Alice can only get 1/2 probability after using the measurement basis measurement $|HH\rangle, |VV\rangle$ or $|VH\rangle, |HV\rangle$. After Alice measures in Protocol 3.2, it can only be obtained with a probability of 1/2 $|HV\rangle$, $|VH\rangle$ or $|HH\rangle$. Therefore, it can be seen that the sender cannot determine the state of the transmitted qubit alone, so this protocol can resist the participant's attack.

4.2 Measure resend attacks, intercept resend attacks and entanglement measurement attacks

In order to resist the eavesdropper's measurement-retransmission attack and intercept the retransmission attack and the entanglement measurement attack, Alice placed m four-particle cluster states in the CD sequence bit string SB, as the decoyed particles to achieve the purpose of deceiving Eve. The original state of the system is:

$$|\rho_{rot}\rangle_{ABCD}=1/2\,(|VHHH\rangle + |HHVV\rangle + |VVHH\rangle + |VVVV\rangle)_{ABCD} \tag{21}$$

Assuming that Eve attacks the quantum system, the effects of the attack on the qubits $|H\rangle$, $|V\rangle$ are set to:

$$\tau|H\rangle \rightarrow \alpha|HX\rangle + \beta|VX'\rangle \; \tau|V\rangle \rightarrow i|HY\rangle + j|VY'\rangle \tag{22}$$

Then the quantum system state after the attack is:

$|\rho'\rangle=\tau\otimes\tau\otimes\tau\otimes\tau|\rho\rangle$

$=1/2\,[(\alpha|HX\rangle + \beta|VX'\rangle)\otimes(\alpha|HX\rangle + \beta|VX\rangle)\otimes(\alpha|HX\rangle + \beta|VX'\rangle)\otimes(\alpha|HX\rangle + \beta|VX'\rangle) + (\alpha|HX\rangle + \beta|VX'\rangle)\otimes(\alpha|HX\rangle + \beta|VX'\rangle)\otimes(i|HY\rangle + j|VY'\rangle)\otimes(i|HY\rangle + j|VY'\rangle) + (i|HY\rangle + j|VY'\rangle)\otimes(i|HY\rangle + j|VY'\rangle)\otimes(\alpha|HX\rangle + \beta|VX'\rangle)\otimes(\alpha|HX\rangle + \beta|VX'\rangle) + (i|HY\rangle + j|VY'\rangle)\otimes(i|HY\rangle + j|VY'\rangle)\otimes(i|HY\rangle + j|VY'\rangle)\otimes(i|HY\rangle + j|VY'\rangle)]$ (23)

Table 3 can be used to indicate specific result.

Table 3 Each collapse state and the corresponding coefficient

Coefficient	Collapse state a/e	Collapse state *b/f*	Coefficient	Collapse state a/e	Collapse state *b/f*
α^4/β^4	$\|HXHXHXHX\rangle$	$\|VX'VX'VX'VX'\rangle$	j^2i^2	$\|VY'HYHYVY'\rangle$	$\|VY'HYVY'HY\rangle$

$\alpha^3\beta$	$\|HXHXHXVX'\rangle$	$\|HXHXVX'HX\rangle$		$\|HYVY'VY'HY\rangle$	$\|VY'HYHYVY'\rangle$
$\alpha\beta^3$	$\|HXVX'VX'VX'\rangle$	$\|VX'HXVX'VX'\rangle$	j^3i	$\|VY'HYHYVY'\rangle$	$\|VY'HYVY'VY'\rangle$
α^2ij	$\|HXHXHYHY\rangle$	$\|HXHXVY'VY\rangle$	$\alpha^3\beta$	$\|HXVX'HXHX\rangle$	$\|VX'HXHXHX\rangle$
$\alpha\beta i^2$	$\|HXHXHYVY'\rangle$	$\|HXHXVY'HY\rangle$	$\alpha^2\beta^2/\alpha^2ij$	$\|HXVX'VX'HX\rangle$	$\|HXHXVY'HY\rangle$
$\alpha\beta ij$	$\|HXVX'HYHY\rangle$	$\|VX'HXHYHY\rangle$	$\alpha\beta^3$	$\|VX'VX'HXVX'\rangle$	$\|VX'VX'VX'HX\rangle$
$\alpha\beta j^2$	$\|HXVX'HYVY'\rangle$	$\|VX'HXHYVY'\rangle$	$\alpha\beta ij/\alpha\beta j^2$	$\|VX'HXVY'HY\rangle$	$\|VX'HXVY'VY'\rangle$
β^2i^2/β^2j^2	$\|HXVX'VY'VY'\rangle$	$\|HXVX'VY'HY\rangle$	$j^4/\ i^3n$	$\|VY'VY'VY'VY'\rangle$	$\|HYHYHYVY'\rangle$
β^2ij	$\|VX'VX'HYHY\rangle$	$\|VX'VX'VYVY\rangle$	i^2j^2	$\|HYVY'VY'HY\rangle$	$\|HYVY'HYVY'\rangle$
i^3n	$\|VX'VX'HYVY\rangle$	$\|VX'VX'VY'HY\rangle$	i^3j	$\|HYHYVY'HY\rangle$	$\|HYVY'HYHY\rangle$
i^2j^2	$\|HYHYHYHY\rangle$	$\|HYHYHYHY\rangle$	ij^3	$\|VY'VY'VY'HY\rangle$	
i^3j	$\|HYHYHYVY'\rangle$	$\|HYHYVY'HY\rangle$	j^2i^2	$\|VY'VY'HYHY\rangle$	$\|HYHYVY'VY'\rangle$
	$\|VY'HYHYHY\rangle$			$\|VY'HYVY'HY\rangle$	$\|VY'VY'HYHY\rangle$
ij^3	$\|HYVY'VY'VY'\rangle$	$\|VY'VY'HYHY\rangle$	j^3i	$\|HYVY'VY'VY'\rangle$	$\|VY'VY'HYVY'\rangle$
$\alpha^2\beta^2$ $\beta^2\alpha^2$	$\|HXHXVX'VX'\rangle$ $\|VX'HXHXVX'\rangle$		$\alpha\beta^3$	$\|HXVX'VX'VX'\rangle$	$\|VX'HXVX'VX'\rangle$

From the above table, the probability that this protocol will resist the success of the attack can be calculated. According to the normality law of the quantum state wave function, it can be known that:

$$|\alpha|^2+|\beta|^2=1,\ \ |i|^2+|j|^2=1 \tag{24}$$

Let $A=|\alpha|^2$, $B=|\beta|^2$, $\mu=|i|^2$, $\eta=|j|^2$, from which we can get the probability that Alice correctly obtains the quantum state:

$$P_1=1/4(A^4+2A^2B^2+A^2X^2+A^2\eta^2+B^2\mu^2+B^2\eta^2+\mu^2+\mu^2\eta^2+\eta^4) \tag{25}$$

According to $B=1-A$, $\eta=1-\mu$, then we can get:

$$P_1=1/4[A^4+2A^2(1-A^2)+A^2X^2+A^2(1-\mu^2)+(1-A^2)\mu^2+(1-A^2)(1-\mu^2)+\mu^4+\mu^2(1-\mu^2)+(1-\mu^2)^2] \tag{26}$$

The mutual information amount of the binary channel Shannon entropy can be obtained by calculation:

$$H(a)=I_{|0\rangle}=-\ a\log_2 a-(1-a)\log_2(1-a)$$

$$H(b)=I_{|1\rangle}=-\ b\log_2 b-(1-b)\log_2(1-b) \tag{27}$$

Since in the binary channel, the maximum information contained in the binary information corresponding to the Shannon entropy is the amount of information contained in one qubit. Let a=b, then A=B=1/4， η=μ=1/2.

Therefore, the result is P_1=56.2%, that is, the probability that Eve attacks and is perceived by both parties of communication is P_2= 43.8%.

4.3 Trojan horse attack

Since each particle in this protocol only needs to be transmitted once, the adversary cannot successfully perform the invisible eavesdropping [12] and the delayed photon Trojan eavesdropping [13].

4.4 Double C-NOT attack

In this protocol, Alice sends a C-NOT attack to the photon sequence in the quantum state sent to Bob due to the random incorporation of decoy particles:

$$|C_1\rangle|C_2\rangle|E\rangle \xrightarrow{C_{C_1E},\ C_{C_2E}} |C_1\rangle|C_2\rangle|E\oplus C_2\oplus C_2\rangle$$

$$|D_1\rangle|D_2\rangle|E\rangle \xrightarrow{C_{D_1E},\ C_{D_2E}} |D_1\rangle|D_2\rangle|E\oplus D_2\oplus D_2\rangle \quad (28)$$

Since Alice has already incorporated the decoupling particles in the sequence S_B before this, the data of the sequence received by Bob is not in one-to-one correspondence with the correct data sequence. Therefore, after Alice uses the Z-based measurement in the protocol, Eve can only get 25% of the secret key after eavesdropping, and the probability of Eve eavesdropping being discovered is 43.8% due to the presence of decoy particles.

5. Efficiency analysis

5.1 Information theory efficiency

The information theory efficiency of the QKA protocol [14] can be expressed as $\lambda_1=b_s/(q_t+b_t)$=61%, where b_s represents the transmitted key bits, b_t represents the classical bits transmitted by both parties, and q_t represents the quantum bits used for negotiation. And the efficiency of the quantum cryptographic protocol against the collective phase-out noise protocol and the anti-collective rotation noise protocol are the same in this protocol. And it is more efficient than the currently existing protocol with a efficiency of 16.6% [15] and a protocol with an efficiency of 10% [16].

5.2 Quantum bit efficiency

The qubit efficiency [17] of the two QKA protocols in this paper is defined as $\lambda_2=q_u/q_t$=33.3%, where q_u denotes the classical bits passed by negotiation, and q_t is the qubit used for negotiation.

6. Conclusion

In this paper, a quantum key distribution protocol based on four-particle entangled W-state is proposed. Both of them can transmit information directly through Z-based quantum measurement, and can eliminate the influence of channel noise on data transmission. At the same time, the detection rate of this protocol can reach 43.8% per qubit, and the information theory efficiency is also improved compared with the previous agreement

References

[1] X.W. WANG，Y.G. SHAN，L.X. XIA, et a1: Dense coding and teleportation with one—dimensional cluster states, Physics Letters A, 2007 364(1): 7—11.

[2] Z.H. Peng, J. Zou, X.J. Liu: Scheme for implementing efficient quantum information processing with multiqubit w-class states in cavity qed, Journal of Physics B: Atomic, Molecular and Optical Physics, 2008 41(6), 065505.

[3] J. Lee, H. Min, S. D. Oh: Multipartite entanglement for entanglement teleportation, Physical Review A, 2002 66(5):357-364.

[4] R. Raussendorf，H.J. Briegel: A One—Way Quantum Computer[J]. Physical Review Letters，2001 86(22): 5188 5191.
[5] F. Verstraete, J. Dehaene, De.Moor. B et a1: Four qubits can be entangled in nine different ways, Physical Review A, 2002 65(5): 052112.
[6] RENE, HEILMANN, MARKUS, et al: A novel integrated quantum circuit for high-order W-state generation and its highly precise characterization, Chinese Science Bulletin, 2015 60(1):96-100.
[7] Bennett.C. H, Brasarrd. G: Quantum Cryptography: Public Key Distribution and Coin Tossing, Proc. IEEE International Conference on Computers Systems and Signal Processing (IEEE, US, 1984), p.175-179.
[8] X.B. WANG: Fault tolerant quantum key distribution protocol with collective random unitary noise, Physical Review A, 2004 72(5):762-776.
[9] X.H. LI, F.G. Deng, H.Y. Zhou: Efficient quantum key distribution over a collective noise channel, Physical Review A, 2008 78(2):-.
[10] F. GAO, S.J. QIN, Q.Y. Wen, et al: Cryptanalysis of multiparty controlled quantum secure direct communication using Greenberger–Horne–Zeilingerstate, Optics Communications, 2010 283(1):192-195.
[11] J. LI, X.J. GUO, D.J. SONG, et al: Improved Quantum "Ping-Pong" Protocol Based on Extended Three-Particle GHz State, China Communications, 2012 9(1):111-116.
[12] Q.Y. CAI: Eavesdropping on the two-way quantum communication protocols with invisible photons, Physics Letters A, 2006 351(1–2):23-25.
[13] F.G. DENG, X.H. Li, H.Y. Zhou, et al: Erratum: Improving the security of multiparty quantum secret sharing against Trojan horse attack, Physical Review A, 2005, 72(4):440-450.
[14] T.Y. YE: Robust quantum dialogue based on logical qubits and controlled-not operations, ScientiaSinica, 2015 45(3):030301.
[15] W. HUANG, Q.Y. WEN, B. LIU, et al: Quantum key agreement with EPR pairs and single-particle measurements, Quantum Information Processing, 2014 13(3):649-663.
[16] W. HUANG, Q. SU, X. WU, et al: Quantum Key Agreement Against Collective Decoherence, International Journal of Theoretical Physics, 2014 53(9):2891-2901.
[17] A. Fahmi, M. Golshani. Comment on: "Quantum key distribution in the Holevo limit" [Phys. Rev. Lett 85 (2000), no. 26, 5635–5638] by A. Cabello, Physical Review Letters, 2000 85(1):5635-8.