


# Measurement-device-independent quantum dialogue

Guo-Fang Shi(石国芳)

**Citation:**Chin. Phys. B, 2021, 30 (**10**): 100303. DOI: 10.1088/1674-1056/ac140a
Journal homepage: http://cpb.iphy.ac.cn; http://iopscience.iop.org/cpb

**What follows is a list of articles you may be interested in**

---

## Fault tolerant controlled quantum dialogue against collective noise

Li-Wei Chang(常利伟), Yu-Qing Zhang(张宇青), Xiao-Xiong Tian(田晓雄), Yu-Hua Qian(钱宇华), Shi-Hui Zheng(郑世慧)

Chin. Phys. B, 2020, 29 (**1**): 010304. DOI: 10.1088/1674-1056/ab5786

## Generating EPR-entangled mechanical state via feeding finite-bandwidth squeezed light

Cheng-qian Yi(伊程前), Zhen Yi(伊珍), Wen-ju Gu(谷文举)

Chin. Phys. B, 2017, 26 (**6**): 060303. DOI: 10.1088/1674-1056/26/6/060303

## Decoherence suppression for three-qubit W-like state using weak measurement and iteration method

Guang Yang(杨光), Bao-Wang Lian(廉保旺), Min Nie(聂敏)

Chin. Phys. B, 2016, 25 (**8**): 080310. DOI: 10.1088/1674-1056/25/8/080310

## Entanglement properties between two atoms in the binomial optical field interacting with two entangled atoms

Tang-Kun Liu(刘堂昆), Kang-Long Zhang(张康隆), Yu Tao(陶宇), Chuan-Jia Shan(单传家), Ji-Bing Liu(刘继兵)

Chin. Phys. B, 2016, 25 (**7**): 070304. DOI: 10.1088/1674-1056/25/7/070304

## Generation of multiparticle three-dimensional entanglement state via adiabatic passage

Wu Xi, Chen Zhi-Hua, Ye Ming-Yong, Chen Yue-Hua, Lin Xiu-Min

Chin. Phys. B, 2013, 22 (**4**): 040309. DOI: 10.1088/1674-1056/22/4/040309

---

# Measurement-device-independent quantum dialogue

Guo-Fang Shi(石国芳)†

*School of Science, Xi'an University of Posts and Telecommunications, Xi'an* 710061, *China*

(Received 23 April 2021; revised manuscript received 20 June 2021; accepted manuscript online 14 July 2021)

Recently, measurement-device-independent quantum secure direct communication schemes were proposed by Niu *et al.* [*Sci. Bull.* **63** 1345 (2018)] and Zhou *et al.* [*Sci. China-Phys. Mech. Astron.* **63** 230362 (2020)]. Inspired by their ideas, in this paper, a measurement-device-independent quantum dialogue protocol based on entanglement is designed and proven to be secure. The advantage of this scheme is that it can not only allow two communicators to transmit secret messages between each other, making the application scenarios more extensive, but can also eliminate all the security loopholes related to the measurement device and information leakage. In terms of experimental implementation, the scheme mainly involves the preparation of entangled states, the preparation of single photons, quantum storage, Bell measurement and other technologies, all of which are mature at present, therefore, the scheme is feasible by using current technologies.

**Keywords:** quantum dialogue, entanglement state, Bell measurement

**PACS:** 03.67.Hk, 03.67.Dd **DOI:** 10.1088/1674-1056/ac140a

## 1. Introduction

Quantum communication is a new way to communicate by using the principles of quantum mechanics. Its security does not depend on the computational complexity in mathematics, but is guaranteed by the physical principles, and is absolutely secure. Quantum communication mainly includes quantum key distribution (QKD), quantum secure direct communication (QSDC), quantum secret sharing (QSS), etc.

The task of QKD[1–3] is that it enables legitimate communicators to establish and share a secret key to encrypt and decrypt messages. Since the first QKD protocol based on a single-photon system was proposed by Bennett and Brassard in 1984 (BB84 protocol),[1] many excellent protocols[2,3] have been put forward successively. Although QKD has the advantage of unconditional security in theory, it still provides potential opportunities for some eavesdropping behaviors[4–8] due to the imperfections of various devices in practical application. Among these imperfections, the defect of measurement equipment is particularly prominent. The solution to this problem is to build a nearly perfect device, which is obviously impractical. Fortunately, in 2012, Lo, Curty and Qi, three researchers, proposed a measurement-device-independent QKD (MID QKD) protocol,[9] which is independent of measurement devices. This QKD system is very different from the previous QKD scheme; that is, all the photons are measured by an untrusted third party. Such a system can be immune to all malicious attacks associated with measurement devices, and it will play a vital role in the development of QKD under real conditions in the future. Moreover, since the third party is in the middle of the two communication parties in the scheme, it can effectively extend the transmission distance of the QKD. All these remarkable advantages make this MID QKD one of the best candidates among all kinds of QKD protocols. It attracted the attention of many researchers as soon as it was reported, and has been an important research topic in recent years.[10–12]

QSDC is another important branch of quantum communication developed in the past 20 years.[13–21] It is a unique technology, which can transmit confidential information directly without the help of secret key and ciphertext. Early QSDC was a one-way transmission of secret information, in 2004, Nguyen first generalized it to a two-way situation, so-called quantum dialogue.[22] This is a very interesting concept, in which Alice and Bob can send secret information each other. Since then, quantum dialogue has gradually grown and attracted lots of attention. However, in 2008, Gao *et al.*[23] and Tan *et al.*[24] independently demonstrated that the quantum dialogue protocol[22] has the drawback of "secret information leakage" from the perspective of information theory, which does not meet the requirements of secure communication. Any secure bidirectional quantum communication protocol or quantum dialogue scheme should not only resist the conventional attacks of eavesdropper, but also avoid the defect of "secret information leakage".[25–27]

Recently, Niu *et al.*[28] and Zhou *et al.*[29] have presented the MID QSDC protocols. Inspired by their ideas, in this paper, we will design a MID quantum dialogue. In this protocol, Alice prepares N identical entangled EPR pairs as quantum channels, Bob prepares entangled EPR pairs according to his own secret information, and both communication parties send their photons sequences to the third party Charlie by means of the quantum data block transmission.[14–16] After a series of security tests, if the channel is secure, Alice will perform the Bell measurement and publish the results. The secret of Bob

†Corresponding author. E-mail: 55310518@qq.com

© 2021 Chinese Physical Society and IOP Publishing Ltd 

is transmitted to Alice by means of teleportation, and the secret of Alice is decoded by Bob with the knowledge of dense coding, thus, quantum dialogue is realized successfully. The security analysis shows that this scheme can not only effectively resist common attacks by eavesdroppers, but also avoid the defect of "secret information leakage". Due to the use of the technology of MID, it can also be immune to all security loopholes associated with the measurement device. Compared with the previous MID quantum dialogue,[27] it is more concise and has higher communication efficiency. Besides, it is feasible with present-day technology.

## 2. Measurement-device-independent quantum dialogue scheme

An EPR pair is a commonly used pair of entangled photons in quantum communication, and its state is one of the following:

$$\begin{aligned}\left|\varphi^{\pm}\right\rangle &= \frac{1}{\sqrt{2}}(|00\rangle \pm |11\rangle),\\ \left|\psi^{\pm}\right\rangle &= \frac{1}{\sqrt{2}}(|01\rangle \pm |10\rangle).\end{aligned} \tag{1}$$

Here 0 and 1 represent the horizontal and vertical polarization states of the photon. In this scheme, two communication parties agree that Bob prepares different quantum states according to the classic secret information bit 0 or 1 he wants to send. The specific corresponding relationship is

$$\begin{aligned}\left|\varphi^{+}\right\rangle \ \text{or}\ \left|\varphi^{-}\right\rangle &\to 0,\\ \left|\psi^{+}\right\rangle \ \text{or}\ \left|\psi^{-}\right\rangle &\to 1.\end{aligned} \tag{2}$$

Alice's secret information will be encoded by a unitary operation, and the corresponding relationship is

$$\begin{aligned}\mathrm{I}\ \text{or}\ \sigma_x &\to 0,\\ \mathrm{i}\sigma_y\ \text{or}\ \sigma_z &\to 1.\end{aligned} \tag{3}$$

The specific scheme consists of the following seven steps, as shown in Fig. 1.

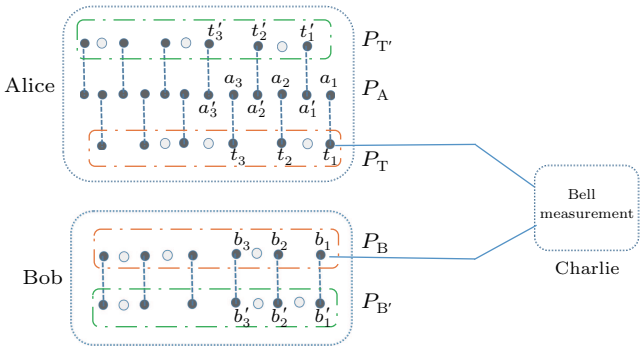



**Fig. 1.** The illustration of MID quantum dialogue scheme. The black photon pairs $(a_1,t_1)(a_1',t_1')(a_2,t_2)(a_2',t_2')\cdots(a_N,t_N)(a_N',t_N')$ at Alice's side are the EPR state $|\varphi^+\rangle_{at}$ in Eq. (1). The black photon pairs $(b_1,b_1'),(b_2,b_2')\cdots(b_N,b_N')$ prepared by Bob are one of EPR states according to Eqs. (1) and (2). The grey single-photon qubits are randomly prepared in one of the BB84 states $\left\{|0\rangle,|1\rangle,|+\rangle=\frac{1}{\sqrt{2}}(|0\rangle+|1\rangle),|-\rangle=\frac{1}{\sqrt{2}}(|0\rangle-|1\rangle)\right\}$.

Step 1: Alice and Bob prepare some ordered photon sequences. Alice prepares $2N$ entangled photon pairs $(a_1,t_1)(a_1',t_1')(a_2,t_2)(a_2',t_2')\cdots(a_N,t_N)(a_N',t_N')$ in $|\varphi^+\rangle_{at}$. She selects $N$ photons $t_1,t_2,\ldots,t_N$ in the entangled pairs to form a sequence $S_T$, the $N$ photons $t_1',t_2',\ldots,t_N'$ in the corresponding order form a sequence $S_{T'}$, and the remaining $2N$ photons $a_1,a_1',a_2,a_2',\ldots,a_N,a_N'$ form a sequence $S_A$ in the same order. In order to perform the subsequent security test, Alice also prepares $2m$ single-photons, randomly in BB84 state $\{|0\rangle,|1\rangle,|+\rangle=\frac{1}{\sqrt{2}}(|0\rangle+|1\rangle),|-\rangle=\frac{1}{\sqrt{2}}(|0\rangle-|1\rangle)\}$, and then inserts them into the random positions of the above sequence $S_T$ and $S_{T'}$, thus Alice has sequences $P_T,P_{T'}$ with the length of $N+m$ single photons, and the sequence of $P_A$ with the length of $2N$ photons.

Bob prepares EPR pairs $(b_1,b_1'),(b_2,b_2')\cdots(b_N,b_N')$ according to his secret message and the agreement in Eq. (2). Similarly, he separates the corresponding photon pairs $b_i$ and $b_i'$ to form an ordered sequence $S_B$ and $S_{B'}$. Finally, he places $m$ single photons in BB84 state at random positions of the sequence $S_B$ and $S_{B'}$ respectively, thus two photon sequences $P_B$ and $P_{B'}$ are generated with the length of $N+m$ photons.

Step 2: Alice and Bob send their respective sequence $P_T$ and $P_B$ to Charlie, the third party located in the middle of the communication line, and keep the $P_{T'}$, $P_A$ and $P_{B'}$ in their hands. Charlie collects the corresponding photons in the sequences $P_T$ and $P_B$ according to their positions, then performs the Bell measurements on $(t_i,b_i)$ in turn and publishes the measurement results.

Step 3: The first security checking. After Charlie announces the Bell measurement outcomes, Alice and Bob announce the specific locations of the single photons in their sequences through classical communication. The source of the photon pairs in Charlie's hand can be divided into three situations, as shown in Table 1.

**Table 1.** The source of photon pairs $(t_i,b_i)$ and the use of Bell measurements in every situation.

| Every situation | Source of $t_i$ | Source of $b_i$ | Functions |
|---|---|---|---|
| (1) | entanglement | entanglement | entanglement swapping for teleportation |
| (2) | single photon | single photon | security checking |
| (3) | single photon | entanglement | discard |
| | entanglement | single photon | discard |

In Table 1, two photons in case (1) are both from the entangled pair of Alice and Bob, and Charlie's Bell measurement is equivalent to allowing the photons in different entangled pairs to achieve entanglement swapping. Such photon pairs are most cases, and will be used to realize quantum dialogue. The photon pairs in case (3) will be discarded because only a

small number of single photons are inserted. In order to make the security test effective, Alice and Bob only use the photons in case (2) to analyze the security of the step 2. The details are as follows:

$$|+\rangle|0\rangle = \frac{1}{2}|\varphi^+\rangle + \frac{1}{2}|\varphi^-\rangle + \frac{1}{2}|\psi^+\rangle + \frac{1}{2}|\psi^-\rangle, \tag{4}$$

$$|-\rangle|1\rangle = -\frac{1}{2}|\varphi^+\rangle + \frac{1}{2}|\varphi^-\rangle + \frac{1}{2}|\psi^+\rangle + \frac{1}{2}|\psi^-\rangle, \tag{5}$$

$$|00\rangle = \frac{1}{\sqrt{2}}\left(|\varphi^+\rangle + |\varphi^-\rangle\right),$$

$$|10\rangle = \frac{1}{\sqrt{2}}\left(|\psi^+\rangle - |\psi^-\rangle\right), \tag{6}$$

$$|++\rangle = \frac{1}{\sqrt{2}}\left(|\varphi^+\rangle + |\psi^+\rangle\right),$$

$$|-+\rangle = \frac{1}{\sqrt{2}}\left(|\varphi^-\rangle + |\psi^-\rangle\right). \tag{7}$$

Alice and Bob exchange the basis information and quantum state of single photons through classical communication. For those single photons with different preparation basis, Bell measurement will lead to any one of four Bell states, as shown in Eqs. (4) and (5), it is not useful for security check and analysis. The decomposition of two photons with identical basis in terms of Bell state are shown as Eqs. (6) and (7), and there are only two possible Bell states. Using these single photons with the same basis, Alice and Bob can estimate that the transmission in Step 2 is secure or not. Such a security check is completely equivalent to the literature,[9] and can also be regarded as the "time reversal" of the QKD protocol (BBM92).[3] The behavior of the eavesdropper Eve would cause some errors when he chooses the wrong measurement basis. Alice and Bob compare and analyze, if the error rate is higher than a threshold, it indicates that Step 2 is insecure, and both parties abandon the above transmission and start again. If they confirm that the quantum channel is safe, then the next step is started.

Step 4: Alice and Bob send their sequence $P_{T'}$ and $P_{B'}$ to Charlie. Charlie collects the corresponding photons from the sequence $P_{T'}$ and $P_{B'}$, then performs the Bell measurements on $(t'_1,b'_1),(t'_2,b'_2)\cdots(t'_{N+m},b'_{N+m})$ and publishes the outcomes.

Step 5: The second security checking. After Charlie publishes the Bell measurement results, Alice and Bob announce the specific positions of the single photons they place in the sequence $P_{T'}$ and $P_{B'}$ by means of classic communication. The security check process is completely similar to Step 3. The photon pairs $(t'_i,b'_i)$ in Charlie's hand are still divided into three types as in table 1. For the case (2) in Table 1, they abandon single photons with different preparation bases and expose single photons with the same preparation bases for security check, they estimate the error rate in the channel and decide whether continue to the communication or not.

Step 6: Alice encodes her secret message. If both parties confirm that the channel is secure, Alice applies unitary operation to encrypt her secret message. After two Bell measurements in Step 3 and Step 5, most of the $N$ photon pairs $(a_1,a'_1),(a_2,a'_2),(a_3,a'_3)\cdots(a_N,a'_N)$ in Alice's hand are the teleportation of EPR pair $(b_1,b'_1),(b_2,b'_2)\cdots(b_N,b'_N)$ (that is, the case 1 in Table 1), however, there are still a small number of pairs caused by the case 3 in Table 1 that are not entangled. Alice discards the pairs of unentangled photons and encodes her own secret information on the remaining $N-\delta$ pairs of entangled photons $(a_j,a'_j)$.

First, Alice performs proper unitary operation $U_T$ on the photon $a_j$ according to Charlie's two Bell measurement outcomes, the specific form of $U_T$ is shown in Table 2, and thus Bob's initial state $(b_j,b'_j)$ can be restored at the side of Alice $(U_T a_j,a'_j)$; second, Alice encodes her secret message by applying unitary operations $U_M$ in accordance with the agreement as shown in Eq. (3). The photon pair in her hand becomes $(U_M U_T a_j,a'_j)$.

Step 7: Alice and Bob extract their secret messages. Usually in the MID quantum communication protocols,[9,27,28] all the Bell measurements are performed by the untrusted third relay Charlie, and two photons from an independent laser source interfere at Charlie's side. In this scheme, after Step 6, what Alice owns is a photon pair $(U_M U_T a_j,a'_j)$, which is not only an entangled Bell state, but also carries the secret information of both parties. In view of this, in this scheme, it is unnecessary for Alice to send photon sequences $U_M U_T a_j$ $(1\le j\le N-\delta)$ and $a'_j$ $(1\le j\le N-\delta)$ to Charlie in two steps and carries out security checks. Here we can adopt a relatively simple method. Instead of Charlie, Alice performs Bell measurement on each photon pair $(U_M U_T a_j,a'_j)$ and publishes the outcome to Bob. This can not only reduce the loss of photons in the transmission of each sequence, but also avoid security analysis, which is obviously very convenient.

**Table 2.** Suppose Bob's third secret is 1 and he prepares initial state $|\psi^-\rangle_{b_3b'_3}$. $U_T$ is a unitary operation to realize the teleportation of $(b_3,b'_3)$ to $(a_3,a'_3)$. The correspondence between Bell measurement outcomes $(t_3,b_3)$, $(t'_3,b'_3)$ of Charlie and $U_T$ performed by Alice.

| The initial state of Bob | Measurement results of Charlie | $U_T$ | Measurement results of Charlie | $U_T$ |
|---|---|---|---|---|
| $\|\psi^-\rangle_{b_3b'_3}$ | $\|\varphi^+\rangle\|\varphi^+\rangle,\|\varphi^-\rangle\|\varphi^-\rangle$<br>$\|\psi^+\rangle\|\psi^+\rangle,\|\psi^-\rangle\|\psi^-\rangle$ | $I$ | $\|\varphi^+\rangle\|\varphi^-\rangle,\|\varphi^-\rangle\|\varphi^+\rangle$<br>$\|\psi^+\rangle\|\psi^-\rangle,\|\psi^-\rangle\|\psi^+\rangle$ | $\sigma_z$ |
| | $\|\varphi^+\rangle\|\psi^+\rangle,\|\varphi^-\rangle\psi\|^-\rangle$<br>$\|\psi^+\rangle\|\varphi^+\rangle,\|\psi^-\rangle\|\varphi^-\rangle$ | $\sigma_x$ | $\|\varphi^+\rangle\|\psi^-\rangle,\|\varphi^-\rangle\|\psi^+\rangle$<br>$\|\psi^+\rangle\|\varphi^-\rangle,\|\psi^-\rangle\|\varphi^+\rangle$ | $\mathrm{i}\sigma_y$ |

For Alice, from the Bell measurement result $(U_{\rm M}U_{\rm T}a_j, a'_j)$ and $U_{\rm M}$, she can infer the initial state $(b_j, b'_j)$ prepared by Bob and extract Bob's 1-bit classical secret information. For Bob, according to the Bell measurement result of $(U_{\rm M}U_{\rm T}a_j, a'_j)$ and his initial state, he can also extract Alice's 1-bit secret message. The quantum dialogue has been realized. In the MID quantum communication scheme, whether it is based on a single-photon state[9,26,27] or an entangled state as a quantum channel,[28] the Bell measurement equipment has always been an indispensable component. Bell measurement using linear optical elements and single-photon detectors is favored because of its simple structure. Such Bell measurement devices can only distinguish two of the four Bell states, that is, they can only identify Bell states probabilistically. This fact will result in the halving of the efficiency both in the security check and the decoding message process, though it does not affect the security of the protocol. It should be noted that four EPR states must be distinguished completely in the current MID quantum dialogue protocol because the secret information in Step 7 carried by Bell state is 2 bits. That is to say, non-linear optical elements[30–32] should be used to accomplish complete Bell measurement in the present scheme.

## 3. Security analysis of the protocol

Now we will prove the security of this protocol.

In the present MID quantum dialogue protocol, it can be seen that the security of the scheme depends on the transmission of the sequences $P_{\rm T}, P_{\rm B}$ and $P_{\rm T'}, P_{\rm B'}$. Both the untrusted third party Charlie and the outside eavesdropper Eve want to get the information of Alice and Bob, and what they want most is the sequence $P_{\rm B}$ and $P_{\rm B'}$. Once they know the state of $(b_j, b'_j)$, they can extract the information of Alice and Bob after Step 7. To achieve this goal, they may adopt two kinds of eavesdropping strategies below.

(1) **Measure-resend attack** During the transmission of the sequence $P_{\rm T}, P_{\rm B}$ in Step 2 (also the sequence $P_{\rm T'}, P_{\rm B'}$ in Step 4), Eve intercepts the photons $b_j$ in sequence $P_{\rm B}$ (also sequence $P_{\rm B'}$), then performs single-photon measurement and resends it to Charlie. However, such eavesdropping will be detected in Step 3 (also Step 5). In sequence $P_{\rm B}$ (and $P_{\rm B'}$), not only sequence $S_{\rm B}$ (and $S_{\rm B'}$) is sent to Charlie, but also BB84 single photons $\left\{|0\rangle, |1\rangle, |+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), |-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)\right\}$ are placed in random positions. Eve is unable to identify which positions are single photons. If a sample single photon is measured and that wrong measurement basis is selected, Eve's eavesdropping behavior will be found in Step 3 (also in Step 5) because the relation in Eqs. (6) and (7) is not satisfied. Similarly, if Eve measures and resends photons in sequences $P_{\rm T}, P_{\rm T'}$ to Charlie, his action can also be detected in Step 3 (and Step 5). By using these sample single photons with the same preparation basis and Bell measurement outcome of Charlie, Alice and Bob can estimate whether it is safe or not during the transmission of $P_{\rm T}, P_{\rm B}$ in Step 2 (also the sequence $P_{\rm T'}, P_{\rm B'}$ in Step 4). This method is equivalent to the security test of the MID QKD protocol,[9] and can be attributed to the time reversal of the BBM92 QKD protocol.

(2) **Fake Bell measurement attack** In Step 2 (and Step 4), Charlie does not perform Bell measurement on the corresponding photons $(t_j, b_j)$ $((t'_j, b'_j))$, but announces a fake Bell measurement result. He keeps the photon $b_j$ unchanged and then collects the corresponding photon pair $(b_j, b'_j)$ after Step 4. By performing the Bell measurement on photon pair $(b_j, b'_j)$, Charlie can extract Bob's secret information.

However, such an attack will also be detected in the security check process of Step 3 and Step 5 because BB84 single photons are randomly inserted in the sequence $P_{\rm T}, P_{\rm B}$ and $P_{\rm T'}, P_{\rm B'}$. If Charlie publishes the fake Bell measurement result of $(t_j, b_j)$ $((t'_j, b'_j))$, there will be a mismatch between his announcement and the possible Bell measurement outcome of sample single photons, i.e., Eqs. (6) and (7), thus the eavesdropping action can be found by legitimate communicators in Step 3 (and Step 5).

Based on the above security analysis, it can be seen that the sample BB84 single photons and the security check in Step 3 and Step 5 are effective in detecting the possible attacks by eavesdroppers. In the following, we will prove the drawback of "secret information leakage" can be eliminated in our MID quantum dialogue.

In this protocol, the photon sequences $P_{\rm T}, P_{\rm B}$ and $P_{\rm T'}, P_{\rm B'}$ are transmitted to Charlie in two steps, and sample single photons are placed in every sequence for the security check. If the channel is confirmed to be safe after the security test of Step 3 and Step 5, the attacker Eve or Charlie cannot obtain any information of the photon pair $(b_j, b'_j)$. The initial quantum state $(b_j, b'_j)$ prepared by Bob has been safely teleported to Alice's photon pair $(a_j, a'_j)$ except for one rotation operation $U_{\rm T}$. It is step-by-step transmission that guarantees that the quantum dialogue protocol does not have the defect of "secret information leakage". For clarity, we will give an example below.

For instance, Bob's third secret bit is 1, and Alice's secret information is 1. From the agreement in Eqs. (2) and (3), Bob prepares the initial state $(b_3, b'_3)$ as $|\psi^-\rangle_{b_3 b'_3}$. Assuming Charlie's Bell measurement result is $|\varphi^+\rangle_{t_3 b_3}|\psi^+\rangle_{t'_3 b'_3}$, Alice first operates $U_{\rm T} = \sigma_x$ on photon $a_3$ according to Table 2, and then performs a unitary transformation $i\sigma_y$ to encode her secret bit 1. Finally she carries out Bell measurement and publishes the outcome $|\varphi^+\rangle_{a_3 a'_3}$. Once the measurement result is published, Alice can infer the initial state prepared by Bob $|\psi^-\rangle_{b_3 b'_3}$ to extract the secret bit "1"; meanwhile, Bob infers Alice's unitary operation $\sigma_x$ and extracts the secret bit "1". Alice and Bob

can exchange secret information securely because $(b_3, b_3')$ has been retrieved safely at Alice's hand in first five steps. For any eavesdropper Charlie or Eve, he does not know the initial state of Bob except a pure guess. In his opinion, if Bob's initial state is $|\psi^-\rangle_{b_3b_3'}$, then $i\sigma_y$ is encrypted by Alice; if Bob's initial state is $|\psi^+\rangle_{b_3b_3'}$, then $\sigma_x$ is encrypted by Alice; if Bob's initial state $|\varphi^+\rangle_{b_3b_3'}$, then Alice performs the operation $I$; if Bob's initial state $|\varphi^-\rangle_{b_3b_3'}$, the operation performed by Alice is $\sigma_z$. In other words, from the Bell measurement results $|\varphi^+\rangle_{a_3a_3'}$, Charlie or Eve infers that the secret information of Bob and Alice should be one of four situations $(1,1)(1,0)(0,0)(0,1)$. For eavesdroppers, they do not get more help about the secret information from the announcement of Alice, but still rely on random guesses. From the perspective of information theory and cryptography, four uncertainties correspond to 2-bit secret messages which are completely undecrypted to Charlie or Eve, so our protocol does not have the drawback of "secret information leakage".

All in all, our protocol is secure.

## 4. Discussion and conclusion

In summary, we have proposed a MID quantum dialogue protocol based on an entangled state, in which two communicators send their photons to the third relay Charlie by using the quantum data block method. After a series of security tests, if the channel is secure, Alice performs Bell measurement and publishes the measurement results. Bob's secret is transmitted to Alice through teleportation, while Alice's secret is decoded with the knowledge of dense coding. The security analysis shows that this scheme can not only effectively resist common attacks by eavesdroppers, but also avoid the defect of "secret information leakage", therefore, it is a secure MID quantum dialogue scheme. Compared with the previous quantum dialogue schemes,[25,26] it eliminates all attacks associated with the measurement device under real conditions and greatly enhances the security of communication. Compared with the MID quantum dialogue[27] based on single photons, this paper not only provides the entanglement-based MID quantum dialogue protocol, but also has two advantages. (1) Our scheme is more concise. In scheme,[27] to prepare the single photons with the same basis between two communicators, as the authors stated, their protocol was divided into two parts: the former was BB84 protocol, and the latter was the MID quantum dialogue. In contrast, our protocol does not need the part of QKD in advance, so the whole scheme is more concise. (2) The communication efficiency of our scheme is higher than that in scheme.[27] $\eta=\frac{c}{q_t+c_t}$ is defined as the communication efficiency [33] of a quantum communication scheme, where $c$ is the number of the secret bits, and $q_t$, $c_t$ are the number of transmitted qubits and classical bits, respectively. For the scheme,[27] if non-linear Bell measurement is adopted, when $c=2$, $q_t=q_{\text{key},t}+q_{\text{dialogue},t}$, $c_t=c_{\text{key},t}+c_{\text{dialogue},t}$ are needed, here $q_{\text{key},t}=4$ is used to establish 2-bit key between two legitimate users, and $q_{\text{dialogue},t}=4$ is the transmitted qubits in quantum dialogue scheme. $c_{\text{key},t}=4$ denotes classical information transmitted in BB84 QKD, and $c_{\text{dialogue},t}=4$ stands for the number of transmitted classical bits in quantum dialogue; therefore, the communication efficiency was $\eta=\frac{2}{(4+4)+(4+4)}=\frac{1}{8}$, whereas in our scheme, if a 2-bit secret message is exchanged, $c=2$, only $q_t=6$ and $c_t=6$ are needed, so $\eta=\frac{2}{6+6}=\frac{1}{6}$, which is higher than the scheme.[27] Obviously, our MID quantum dialogue protocol is more advantageous.

Quantum dialogue belongs to the category of QSDC, in the current MID quantum dialogue scheme, it mainly involves Bell state preparation, single photon preparation, quantum storage, Bell state measurement and other technologies, and these technologies have been mature in the experimental realization of QSDC. In 2017, academician Guo guangcan's research group realized an entanglement-based QSDC with the help of atom ensemble quantum memory.[34] In the same year, Zhu *et al.* increased the transmission distance of the entanglement-based QSDC in the optical fiber in the order of kilometers,[35] and achieved long-distance safe communication. In 2020, academician Pan Jianwei and his collaborators realized MID QKD in free space for the first time.[36] All these experimental successes undoubtedly show that the MID quantum dialogue protocol is achievable with current technology.

## References


[1] Bennett C H and Brassard G 1984 *Proc. Int. Conf. on Computers, Systems & Signal Processing*, Bangalore, India, IEEE, New York p. 175
[2] Ekert A K 1991 *Phys. Rev. Lett.* **67** 661
[3] Bennett C H, Brassard G and Mermin N D 1992 *Phys. Rev. Lett.* **68** 557
[4] Fung C H F, Qi B, Tamaki K and Lo H K 2007 *Phys. Rev. A* **75** 032314
[5] Xu F H, Qi B and Lo H K 2010 *New J. Phys.* **12** 113026
[6] Zhao Y, Fung C H F, Qi B, Chen C and Lo H K 2008 *Phys. Rev. A* **78** 042333
[7] Lydersen L, Wiechers C, Wittmann C, Elser D, Skaar J and Makarov V 2010 *Nat. Photon.* **4** 686
[8] Meda A, Degiovanni I P, Tosi A, Yuan Z, Brida G and Genovese M 2017 *Light. Sci. Appl.* **6** e16261
[9] Lo H K, Curty M and Qi B 2012 *Phys. Rev. Lett.* **108** 130503
[10] Sun S H, Gao M, Li C Y and Liang L M 2013 *Phys.Rev. A.* **87** 052329
[11] Xu F H, Curty M, Qi B and Lo H K 2013 *New. Jour. Phys.* **15** 113007
[12] Cui Z X, Zhong W, Zhou L and Sheng Y B 2019 *Sci. China-Phys. Mech. Astron.* **62** 110311
[13] Bostrom K and Felbinger T 2002 *Phys. Rev. Lett.* **89** 187902
[14] Long G L and Liu X S 2002 *Phys. Rev. A* **65** 032302
[15] Deng F G, Long G L and Liu X S 2003 *Phys. Rev. A* **68** 042317
[16] Deng F G and Long G L 2004 *Phys. Rev. A* **69** 052319
[17] Chen S S, Zhou L, Zhong W and Sheng Y B 2018 *Sci. China-Phys. Mech. Astron.* **61** 090312
[18] Li T and Long G L 2020 *New J. Phys.* **22** 063017
[19] Liu D, Chen J L and Jiang W 2012 *Int. J. Theor. Phys.* **51** 2923
[20] Wang C, Deng F G and Long G L 2005 *Opt. Commun.* **253** 15
[21] Gu B, Huang Y G, Fang X and Zhang C Y 2011 *Chin. Phys. B* **20** 100309
[22] Nguyen B A 2004 *Phys. Lett. A* **328** 6
[23] Gao F, Guo F Z, Wen Q Y and Zhu F C 2008 *Sci. China Ser. G Phys. Mech. Astron.* **51** 559
[24] Tan Y G and Cai Q Y 2008 *Int. J. Quant. Inf.* **6** 325

[25] Shi G F, Xi X Q, Tian X L and Yue R H 2009 *Opt. Commun.* **282** 2460
[26] Shi G F, Xi X Q, Hu M L and Yue R H 2010 *Opt. Commun.* **283** 1984
[27] Arpita M 2017 *Quantum. Inf. Process.* **16** 305
[28] Niu P H, Zhou Z R, Lin Z S, Sheng Y B, Liu G Y and Long G L 2018 *Sci. Bull.* **63** 1345
[29] Zhou Z R, Sheng Y B, Niu P H, Liu G Y, Long G L and Hanzo L 2020 *Sci. China-Phys. Mech. Astron.* **63** 230362
[30] Li T, Miranowicz A, Hu X D, Xia K Y and Nori F 2018 *Phys. Rev. A.* **97** 062318
[31] Song G Z, Munro E, Nie W, Kwek L C, Deng F G and Long G L 2018 *Phys. Rev. A* **98** 023814
[32] Qin W, Miranowicz A, Li P B, Lü X Y, You J Q and Nori F 2018 *Phys. Rev. Lett.* **120** 093601
[33] Cabello A 2000 *Phys. Rev. Lett.* **85** 5635
[34] Zhang W, Ding D S, ShengY B, Zhou L, Shi B S and Guo G C 2017 *Phys. Rev. Lett.* **118** 220501
[35] Zhu F, Zhang W, Sheng Y B and Huang Y 2017 *Sci. Bull.* **62** 1519
[36] Cao Y, Li Y H, Yang K X, Jiang Y F, Li S L, Hu X L, Abulizi M, Li C L, Zhang W J, Sun Q C, Liu W Y, Jiang X, Liao S K, Ren J G, Li H, You L X, Wang Z, Yin J, Lu C Y, Wang X B, Zhang Q, Peng C Z and Pan J W 2020 *Phys. Rev. Lett.* **125** 260503