doi:10.3788/gzxb20144303.0327001

# 基于腔 QED 的无信息泄露量子对话

叶天语
(浙江工商大学 信息与电子工程学院,杭州 310018)

**摘 要**:良好的安全性对量子保密通信协议而言是不可或缺的,但信息泄露已成为量子对话的一个严重安全威胁.为了解决信息泄露问题,利用腔 QED 中原子的演化规律提出一个基于腔 QED 的无信息泄露量子对话协议,利用腔 QED 中两个 Bell 态纠缠交换后的测量相关性来克服信息泄露问题.研究表明:该协议能够通过安全检测探测到外部窃听者的主动攻击,如截获-重发攻击、测量-重发攻击和纠缠-测量攻击;在每轮通信可以安全交换 4 比特秘密信息;对信息泄露问题和外部窃听者的主动攻击,都具备良好的安全性.

**关键词**:量子对话;信息泄露;纠缠交换;Bell 态;腔 QED
**中图分类号**:O431.2 **文献标识码**:A **文章编号**:1004-4213(2014)03-0327001-6

# Quantum Dialogue Without Information Leakage via Cavity QED

YE Tian-yu
(*College of Information & Electronic Engineering, Zhejiang Gongshang University, Hangzhou* 310018, *China*)

**Abstract**: Good security is indispensable to any quantum secret communication protocol. However, information leakage has been a great security threat to quantum dialogue. In order to solve the problem, a quantum dialogue protocol without information leakage via cavity QED was proposed, which made full use of the evolution law of atoms in cavity QED. The proposed quantum dialogue protocol avoided the information leakage problem by using the measurement correlation property after entanglement swapping between two Bell states via cavity QED, and could securely exchange 4 bits secret messages per round communication. The results show that the proposed protocol is able to detect the active attacks from the outside eavesdropper through security checking, such as the intercept-resend attack, the measurement-resend attack and the entanglement-and-measurement attack. Therefore, it has good security towards both the information leakage problem and the active attacks from the outside eavesdropper.

**Key words**: Quantum dialogue; Information leakage; Entanglement swapping; Bell state; Cavity QED
**OCIS Codes**: 270.5568; 270.5565; 270.5585

## 0 Introduction

Quantum secure direct communication (QSDC) aims to offer confidential transmission of classic information over a quantum channel without prior key agreement. Until now, a lot of good QSDC protocols[1-10] have been proposed. However, these QSDC protocols were merely message-unilaterally-transmitted communication protocols. Fortunately, in 2014, Zhang *et al*.[11-13] and Nguyen[14] put forward the concept of quantum dialogue, which allows two authorized communication parties to exchange their

**Foundation item**: The National Natural Science Foundation of China (No. 11375152) and the Natural Science Foundation of Zhejiang Province (No. LQ12F02012)
**First author**: YE Tian-yu(1982—), male, associate professor, Ph. D. degree, mainly focuses on quantum cryptography and information hiding. Email:happyyty@aliyun.com
**Received**: Jun. 13, 2013; **Accepted**: Sep. 5, 2013

secret messages simultaneously. In 2005, Man *et al*.[15] pointed out that Nguyen′ protocol[14] is unable to resist the intercept-and-resend attack and gave a solution to this problem. In 2006, Jin *et al*.[16] proposed a three-party simultaneous QSDC using a GHZ state. Man and Xia[17] proposed a controlled bidirectional QSDC by a GHZ state. Man *et al*.[18] put forward a quantum dialogue protocol based on entanglement swapping of GHZ states in the same year. In 2007, Man and Xia[19] pointed out that Jin′s protocol[16] has the problem of definite information leakage and put forward an improved version for it. Chen *et al*.[20] put forward a bidirectional QSDC based on entanglement swapping of Bell sates. Yang and Wen[21] proposed a quasi-secure quantum dialogue protocol using a single photon. In 2008, Gao *et al*.[22] pointed out that both Jin′s protocol[16] and Man′s improved version[19] have the problem of information leakage from the point of information theory and cryptography. Moreover, Gao et al.[23] pointed out that all of Nguyen′s protocol[14], Man′s protocol[15] and Man′s protocol[18] have the problem of information leakage. Unfortunately, Gao *et al*.[22-23] have not suggested how to solve the problem. In 2009, Shan *et al*.[24] put forward a quantum dialogue protocol based on entanglement swapping of two Bell states via cavity QED. In 2013, Ye and Jiang[25] presented two approaches to improve the problem of definite information leakage in Man′s protocol[17]. However, information leakage still happens in Ye′s two protocols[25], as pointed in Refs. [26-27]. In fact, all these protocols[11-13,17,20-21,24] have the problem of information leakage. From the analysis above, it can be concluded that information leakage occurs in most of those existing quantum dialogue protocols so that it has been a great security threat to quantum dialogue. How to solve the problem of information leakage will definitely be a hot study point in the near future. At present, using the auxiliary quantum state and the measurement correlation property after entanglement swapping are the two main approaches to overcome the problem of information leakage in quantum dialogue. In 2009, Shi *et al*.[28] proposed a quantum dialogue protocol based on a Bell state using the auxiliary Bell state to overcome the problem of information leakage. In 2010, Shi *et al*.[29] proposed a quantum dialogue protocol based on a single photon using the auxiliary single photon to overcome the problem of information leakage. Shi[30] presented a bidirectional QSDC without information leakage based on the auxiliary particle and the correlation extractability of Bell states. In the same year, Gao[31] proposed two quantum dialogue protocols without information leakage based on the measurement correlation property after entanglement swapping between two Bell states. In 2013, Ye and Jiang[32] avoided the problem of information leakage in a controlled quantum dialogue by making full use of the measurement correlation property after entanglement swapping between two GHZ states and decreasing the transmission efficiency.

In this paper, the author proposes a quantum dialogue protocol without information leakage via cavity QED, which makes full use of the evolution law of atoms in cavity QED. The proposed protocol overcomes the problem of information leakage by using the measurement correlation property after entanglement swapping between two Bell states via cavity QED. Moreover, the proposed protocol can detect the active attacks from the outside eavesdropper through security checking. Therefore, the security of the proposed protocol can be guaranteed.

## 1 Quantum dialogue protocol

The Bell states are two-atom maximally entangled states, which form a complete orthogonal basis of four-dimensional Hilbert space. The four Bell states can be expressed as follows

$$|\Phi^-\rangle=\frac{1}{\sqrt{2}}(|ee\rangle-i|gg\rangle) \tag{1}$$

$$|\Psi^-\rangle=\frac{1}{\sqrt{2}}(|ge\rangle-i|eg\rangle) \tag{2}$$

$$|\Psi^+\rangle=\frac{1}{\sqrt{2}}(|ge\rangle+i|eg\rangle) \tag{3}$$

$$|\Phi^+\rangle=\frac{1}{\sqrt{2}}(|ee\rangle+i|gg\rangle) \tag{4}$$

where $|e\rangle$ and $|g\rangle$ are the excited and ground states of atom, respectively. $U_{00}=I=|g\rangle\langle g|+|e\rangle\langle e|$, $U_{01}=\sigma_x=|g\rangle\langle e|+|e\rangle\langle g|$, $U_{10}=i\sigma_y=|g\rangle\langle e|-|e\rangle\langle g|$ and $U_{11}=\sigma_z=|g\rangle\langle g|-|e\rangle\langle e|$ are four single-atom unitary operations, where the subscript in each $U$ represents two-bit secret message. That is to say, $I\rightarrow 00$, $\sigma_x\rightarrow 01$, $i\sigma_y\rightarrow 10$ and $\sigma_z\rightarrow 11$. It is obvious that one Bell state can be transformed into another after performed with one of the four single-atom unitary operations on its any atom.

We consider the case that driven by a classical field, two identical two-level atoms simultaneously interact with a single-mode cavity. Under the rotating-wave approximation, the interaction Hamiltonian between the single-mode cavity and the atoms can be described as[24,33-35]

$$H=\omega_0 S_z+\omega_a a^\dagger a+\sum_{j=1}^{2}[g(a^\dagger S_j^-+aS_j^\dagger)+\Omega(S_j^\dagger e^{-i\omega t}+S_j^- e^{i\omega t})] \tag{5}$$

where $S_z=(1/2)\sum_{j=1}^{2}(|e_j\rangle\langle e_j|-|g_j\rangle\langle g_j|)$, $S_j^-=|g_j\rangle$

$\langle e_j|, S_j^+ = |e_j\rangle\langle g_j|$, $|g_j\rangle$ and $|e_j\rangle$ are the ground and excited states of the $j^{\text{th}}$ atom, $g$ is the atom-cavity coupling strength, $a$ and $a^\dagger$ are the annihilation and creation operators for the cavity mode, $\omega_0$, $\omega_a$, $\omega$ and $\Omega$ are the atomic transition frequency, the cavity frequency, the classical field frequency and the Rabi frequency, respectively. Suppose $\omega_0 = \omega$, the evolution operator of the system in the interaction picture can be described as[24,33-35]

$$U(t) = e^{-iH_e t} e^{-iH_r t} \tag{6}$$

where $H_0 = \Omega \sum_{j=1}^{2} (S_j^+ + S_j^-)$, and $H_e$ is the effective Hamiltonian. Considering the large detuning case $\delta \gg g$ ($\delta$ is the detuning between $\omega_0$ and $\omega_a$) and the strong driving regime $\Omega \gg \delta, g$, there is no energy exchange between the atomic system and the cavity. Consequently, the effects of cavity decay and thermal field are eliminated. Then, in the interaction picture, the effective interaction Hamiltonian $H_e$ can be expressed as[24,33-35]

$$H_e = (\lambda/2)\left[\sum_{j=1}^{2}(|e_j\rangle\langle e_j| + |g_j\rangle\langle g_j|) + \sum_{i,j=1,i\neq j}^{2}(S_i^+ S_j^- + S_i^+ S_j^+ + H.C.)\right] \tag{7}$$

where $\lambda = g^2/2\delta$. Suppose that the two atoms are simultaneously sent into the cavity described above, and interact with it driven by a classical field. If the interaction time and Rabi frequency are chosen to satisfy $\lambda t = \pi/4$ and $\Omega t = \pi$, the two atoms will undergo the following evolution

$$|gg\rangle_{jk} \rightarrow \frac{\sqrt{2}}{2} e^{-i\pi/4}(|gg\rangle_{jk} - i|ee\rangle_{jk}) \tag{8}$$

$$|ge\rangle_{jk} \rightarrow \frac{\sqrt{2}}{2} e^{-i\pi/4}(|ge\rangle_{jk} - i|eg\rangle_{jk}) \tag{9}$$

$$|eg\rangle_{jk} \rightarrow \frac{\sqrt{2}}{2} e^{-i\pi/4}(|eg\rangle_{jk} - i|ge\rangle_{jk}) \tag{10}$$

$$|ee\rangle_{jk} \rightarrow \frac{\sqrt{2}}{2} e^{-i\pi/4}(|ee\rangle_{jk} - i|gg\rangle_{jk}) \tag{11}$$

Without loss of generality, assume that both the atoms $A$ and $B$ and the atoms $C$ and $D$ are in the state $|\Psi^-\rangle$. That is to say, it has $|\Psi^-\rangle_{AB}$ and $|\Psi^-\rangle_{CD}$. The atoms $A$ and $C$ are simultaneously sent into the single-mode cavity described above. Driven by a classical field, the atoms $A$ and $C$ simultaneously interact with the single-mode cavity. The interaction time and Rabi frequency are chosen to satisfy $\lambda t = \pi/4$ and $\Omega t = \pi$. It can be verified from Eqs. (8-11) that the whole system will evolve into[24]

$$|\Psi^-\rangle_{AB} \otimes |\Psi^-\rangle_{CD} \rightarrow \frac{1}{2}[-i|ee\rangle_{AC}|\Phi^-\rangle_{BD} - i|eg\rangle_{AC}|\Psi^-\rangle_{BD} - |ge\rangle_{AC}|\Psi^+\rangle_{BD} + |gg\rangle_{AC}|\Phi^+\rangle_{BD}] \tag{12}$$

According to Eq. (12), two initial Bell states collapse to four outcome combinations of the atoms $A$ and $C$ and the atoms $B$ and $D$ each with probability 1/4 after entanglement swapping and evolution. Moreover, the relation between the outcome of the atoms $A$ and $C$ and the outcome of the atoms $B$ and $D$ is highly correlated. In other words, if the outcome of the atoms $A$ and $C$ is $|ee\rangle_{AC}$ ($|eg\rangle_{AC}$, $|ge\rangle_{AC}$, $|gg\rangle_{AC}$), the atoms $B$ and $D$ will collapse to $|\Phi^-\rangle_{BD}$ ($|\Psi^-\rangle_{BD}$, $|\Psi^+\rangle_{BD}$, $|\Phi^+\rangle_{BD}$). It means that one can infer the state of the atoms $B$ and $D$ according to the state of the atoms $A$ and $C$. This character is called as the measurement correlation property after entanglement swapping between two Bell states via cavity QED. This correlation property will be used to design a quantum dialogue protocol without information leakage in this paper.

Suppose that Alice has $2N$ bits secret messages $\{(k_1, l_1)(k_2, l_2)\cdots(k_n, l_n)\cdots(k_N, l_N)\}$, and Bob has $2N$ bits secret messages $\{(i_1, j_1)(i_2, j_2)\cdots(i_n, j_n)\cdots(i_N, j_N)\}$, where $k_t$, $l_t$, $i_t$, $j_t \in \{0,1\}$, $t \in \{1,2,\cdots,n,\cdots,N\}$. Alice and Bob want to exchange their secret messages simultaneously. The proposed quantum dialogue protocol is described in detail as follows.

Step1: Preparation for the initial states and the first round transmission. Alice produces $2N$ Bell states $\{(A_1, B_1), (A_2, B_2), \cdots, (A_{2N}, B_{2N})\}$ all in the state $|\Psi^-\rangle$, where the subscript denotes the order of each Bell state. Atoms $A$ and $B$ from each Bell state form the ordered atom sequences $S_A$ and $S_B$, respectively. In other words, $S_A = \{A_1, A_2, \cdots, A_{2N}\}$ and $S_B = \{B_1, B_2, \cdots, B_{2N}\}$. Alice prepares a large number of single atoms randomly in one of the four states $\{|g\rangle, |e\rangle, |+\rangle, |-\rangle\}$ for the first round security checking, where $|+\rangle = (|g\rangle + |e\rangle)/\sqrt{2}$ and $|-\rangle = (|g\rangle - |e\rangle)/\sqrt{2}$, and randomly inserts these single atoms into sequence $S_B$ to form a new sequence $S_B'$. Then, Alice sends $S_B'$ to Bob.

Step2: The first round security checking. After Bob confirms Alice that he has received sequence $S_B'$, Alice publishes the positions and the corresponding preparation basis of the sample atoms. Then, Bob measures the sample atoms in the same basis as the preparation basis of Alice and tells Alice his measurement outcomes. Alice judges whether there is an eavesdropping by comparing the initial states of the sample atoms with Bob's measurement outcomes. If the error rate goes beyond the threshold, Alice halts the communication; otherwise, the communication goes on.

Step3: Evolution in cavity QED and Bob's encoding. After getting rid of the sample atoms, sequence $S_B'$ turns back into $S_B$. Both Alice and Bob

make the two adjacent atoms from their own atom sequence to form a two-atom group. In other words, $(A_{2n-1},A_{2n})$ and $(B_{2n-1},B_{2n})$ $(n=1,2,\cdots,N)$ are the $n$ th two-atom group from $S_A$ and $S_B$, respectively. Then Alice sends each two-atom group from $S_A$ into the single-mode cavity described above. Driven by a classical field, the two atoms $A_{2n-1}$ and $A_{2n}$ simultaneously interact with the single-mode cavity. Alice chooses the Rabi frequency and the interaction time satisfying $\Omega t=\pi$ and$\lambda t=\pi/4$. Then, Alice detects the states of the two atoms $A_{2n-1}$ and $A_{2n}$ under $Z$-basis $\{|g\rangle,|e\rangle\}$ after they fly out the single-mode cavity. In the meanwhile, Bob performs Bell-basis measurement on each two-atom group $(B_{2n-1},B_{2n})$ from $S_B$. Alice can infer the Bell-basis measurement outcome of $(B_{2n-1},B_{2n})$ according to Eq. (12). According to his Bell-basis measurement outcome, Bob reproduces a new $(B_{2n-1},B_{2n})$ with no state measurement performed. Afterward, Bob performs the unitary operation $U^B_{i_nj_n}$ on the first atom of the new $(B_{2n-1},B_{2n})$ to encode his two-bit secret message. Consequently, $(B_{2n-1},B_{2n})$ turns into $(U^B_{i_nj_n}B_{2n-1},B_{2n})$.

Step4: The second round transmission and the second round security checking. Bob prepares a large number of single atoms randomly in one of the four states $\{|g\rangle,|e\rangle,|+\rangle,|-\rangle\}$ for the second round security checking, and randomly inserts these single atoms into sequence $S_B$ to form a new sequence $S''_B$. Then, Bob sends $S''_B$ to Alice. After Alice confirms Bob that she has received $S''_B$, Bob firstly publishes the positions and the corresponding preparation basis of the sample atoms. Then, Alice measures the sample atoms in the same basis as the preparation basis of Bob and tells Bob her measurement outcomes. Bob judges whether there is an eavesdropping by comparing the initial states of the sample atoms with Alice′s measurement outcomes. If the error rate goes beyond the threshold, Bob halts the communication; otherwise, the communication goes on.

Step5: Quantum dialogue. After getting rid of the sample atoms, sequence $S''_B$ turns back into $S_B$. Now, Alice has two sequences $S_A$ and $S_B$ in her hand. Alice performs the unitary operation $U^A_{k_nl_n}$ on the second atom of $(U^B_{i_nj_n}B_{2n-1},B_{2n})$ to encode her two-bit secret message. Consequently, $(U^B_{i_nj_n}B_{2n-1},B_{2n})$ turns into $(U^B_{i_nj_n}B_{2n-1},U^A_{k_nl_n}B_{2n})$. Then, Alice performs Bell-basis measurement on $(U^B_{i_nj_n}B_{2n-1},U^A_{k_nl_n}B_{2n})$ and publishes its measurement outcome. Therefore, according to his own Bell-basis measurement outcome of $(B_{2n-1},B_{2n})$ and his own unitary operation $U^B_{i_nj_n}$, Bob can infer Alice′s two-bit secret message $(k_n,l_n)$ from Alice′s announcement of $(U^B_{i_nj_n}B_{2n-1},U^A_{k_nl_n}B_{2n})$. On the other hand, according to her own unitary operation $U^A_{k_nl_n}$ and her own measurement outcome of $(U^B_{i_nj_n}B_{2n-1},U^A_{k_nl_n}B_{2n})$, Alice can infer Bob′s two-bit secret message $(i_n,j_n)$, since she can know the Bell-basis measurement result of $(B_{2n-1},B_{2n})$ according to Eq. (12). Until now, the dialogue between Alice and Bob has been finished.

An example is given to further explain the dialogue process. Without loss of generality, we take the $n$ th two-atom groups $(A_{2n-1},A_{2n})$ and $(B_{2n-1},B_{2n})$ for example. Suppose that Alice′s two-bit secret message $(k_n,l_n)$ is 01, and Bob′s two-bit secret message $(i_n,j_n)$ is 10. Alice sends the two atoms $A_{2n-1}$ and $A_{2n}$ into the single-mode cavity and chooses the Rabi frequency and the interaction time satisfying $\Omega t=\pi$ and $\lambda t=\pi/4$. Alice detects the states of the two atoms $A_{2n-1}$ and $A_{2n}$ under $Z$-basis after they fly out the single-mode cavity. In the meanwhile, Bob performs Bell-basis measurement on $(B_{2n-1},B_{2n})$. According to Eq. (12), Alice can infer the state of $(B_{2n-1},B_{2n})$ from the states of the two atoms $A_{2n-1}$ and $A_{2n}$. It is easy to know from Eq. (12) that the states of the atoms $A_{2n-1}$ and $A_{2n}$ and the atoms $B_{2n-1}$ and $B_{2n}$ will collapse to $|ee\rangle_{A_{2n-1}A_{2n}}|\Phi^-\rangle_{B_{2n-1}B_{2n}}$, $|eg\rangle_{A_{2n-1}A_{2n}}|\Psi^-\rangle_{B_{2n-1}B_{2n}}$, $|ge\rangle_{A_{2n-1}A_{2n}}|\Psi^+\rangle_{B_{2n-1}B_{2n}}$ and $|gg\rangle_{A_{2n-1}A_{2n}}|\Phi^+\rangle_{B_{2n-1}B_{2n}}$ each with probability 1/4. According to his Bell-basis measurement outcome, Bob reproduces a new $(B_{2n-1},B_{2n})$ with no state measurement performed. Without loss of generality, assume that the states of the atoms $A_{2n-1}$ and $A_{2n}$ and the atoms $B_{2n-1}$ and $B_{2n}$ collapse to $|ee\rangle_{A_{2n-1}}A_{2n}|\Phi^-\rangle_{B_{2n-1}B_{2n}}$. Bob performs the unitary operation $i\sigma_y$ on the first atom of the new $|\Phi^-\rangle_{B_{2n-1}B_{2n}}$ to encode his two-bit secret message $(i_n,j_n)$. Accordingly, $|\Phi^-\rangle_{B_{2n-1}}B_{2n}$ turns into $|\Psi^+\rangle_{B_{2n-1}B_{2n}}$. After having two sequences $S_A$ and $S_B$ in her hand, Alice performs the unitary operation $\sigma_x$ on the second atom of $|\Psi^+\rangle_{B_{2n-1}B_{2n}}$ to encode her two-bit secret message $(k_n,l_n)$. Consequently, $|\Psi^+\rangle_{B_{2n-1}B_{2n}}$ turns into $|\Phi^+\rangle_{B_{2n-1}B_{2n}}$. Then, Alice performs Bell-basis measurement on $|\Phi^+\rangle_{B_{2n-1}B_{2n}}$ and publishes its measurement outcome. Therefore, according to his own unitary operation $i\sigma_y$, Bob can infer Alice′s two-bit secret message $(k_n,l_n)$ is 01, since his own Bell-basis measurement outcome of $(B_{2n-1},B_{2n})$ is $|\Phi^-\rangle_{B_{2n-1}B_{2n}}$. On the other hand, according to her own unitary operation $\sigma_x$ and her own measurement outcome of $(U^B_{i_nj_n}B_{2n-1},U^A_{k_nl_n}B_{2n})$, Alice can infer that Bob′s two-bit secret message $(i_n,j_n)$ is 10, since she can know that the state of $(B_{2n-1},B_{2n})$ is $|\Phi^-\rangle_{B_{2n-1}B_{2n}}$ by detecting the states of the two atoms $A_{2n-1}$ and $A_{2n}$ under $Z$-basis.

## 2 Security analysis

In the proposed protocol, both the first round and

the second round security checking use the sample atoms randomly prepared in one of the four states $\{|g\rangle,|e\rangle,|+\rangle,|-\rangle\}$ to check the outside eavesdropping. Without loss of generality, take the transmission of sequence $S_B'$ for example to analyze Eve′s active attacks. 1) The intercept-resend attack. Eve intercepts sequence $S_B'$ and sends his fake sequence prepared in advance instead of it to Bob. Since Bob′s measurement outcomes on the fake sequence are not always the same as the genuine ones, Eve will be detected with probability $1/2$[20,25]. 2) The measurement-resend attack. After intercepting sequence $S_B'$, Eve measures it and resends it to Bob. Since Eve′s measurement basis is not always consistent with Alice′s preparation basis, Eve will be detected with probability $1/4$[20,25]. 3) The entanglement-and-measurement attack. Eve may steal partial information by entangling his auxiliary atom $|\varepsilon\rangle$ with the atoms in sequence $S_B'$. Then it follows

$$\begin{aligned}\hat{E}|g\rangle|\varepsilon\rangle&=\alpha_1|g\rangle|\varepsilon_{00}\rangle+\beta_1|e\rangle|\varepsilon_{01}\rangle,\\ \hat{E}|e\rangle|\varepsilon\rangle&=\beta_2|g\rangle|\varepsilon_{10}\rangle+\alpha_2|e\rangle|\varepsilon_{11}\rangle\end{aligned}\tag{13}$$

Apparently, Eve will be detected with probability $\zeta=|\beta_1|^2=|\beta_2|^2$ when the security checking is implemented under $Z$-basis[20,25].

# 3 Discussions

## 3.1 The information leakage problem

Here, the problem of information leakage is analyzed from the perspective of information theory. Due to the measurement correlation property after entanglement swapping between two Bell states via cavity QED, Alice can infer the state of $(B_{2n-1},B_{2n})$ by detecting the states of the two atoms $A_{2n-1}$ and $A_{2n}$ under $Z$-basis after they fly out the single-mode cavity. Therefore, it is not necessary for Bob to publish his Bell-basis measurement outcome of $(B_{2n-1},B_{2n})$ to Alice, which makes Eve have no access to $(B_{2n-1},B_{2n})$. The only thing Eve can do is to purely guess it. Therefore, as to Eve, Alice′s announcement of the measurement outcome of $(U^B_{i_nj_n}B_{2n-1},U^A_{k_nl_n}B_{2n})$ means totally $4\times4$ kinds of unitary operation combinations performed by Alice and Bob. It means that the quantum channel contains $-\sum_{i=1}^{16}p_i\log_2 p_i=-16\times\frac{1}{16}\log_2\frac{1}{16}=4$ bits secret messages for Eve, which is equal to the total amount of secret messages. Therefore, the problem of information leakage is avoided in the proposed protocol. It is easy to know that, the reason why no information has been leaked out in the proposed protocol lies in the measurement correlation property after entanglement swapping between two Bell states via cavity QED.

## 3.2 Comparison with the previous quantum dialogue protocol via cavity QED

A comparison between the proposed protocol and the protocol in Ref. [24] is drawn here, since both of them use entanglement swapping between two Bell states via cavity QED. In Ref. [24], each two Bell states is used to transmit 4 bits secret messages in total, i. e., 2 bits from Alice and 2 bits from Bob. However, 2 bits are leaked out to Eve from the perspective of information theory, which makes the protocol in Ref. [24] essentially unsafe. However, as analyzed above, no information leakage occurs in the proposed protocol. Therefore, with regard to the security, the proposed protocol has better performance than the protocol in Ref. [24].

# 4 Conclusion

In summary, the author propose a quantum dialogue protocol without information leakage via cavity QED, which makes full use of the evolution law of atoms in cavity QED. The proposed protocol avoids the problem of information leakage by using the measurement correlation property after entanglement swapping between two Bell states via cavity QED. Moreover, it can detect the active attacks from the outside eavesdropper through security checking. Therefore, the security of the proposed protocol can be guaranteed.

**References**


[1] BEIGE A, ENGLERT B G, KURTSIEFER C, *et al*. Secure communication with a publicly known key[J]. *Acta Physica Polonica A*, 2002, **101**: 357.

[2] BOSTROM K, FELBINGER T. Deterministic secure direct communication using entanglement [J]. *Physical Review Letters*, 2002, **89**: 187902.

[3] DENG F G, LONG G L, LIU X S. Two-step quantum direct communication protocol using the Einstein-Podolsky-Rosen pair block[J]. *Physical Review A*, 2003, **68**: 042317.

[4] CAI Q Y, LI B W. Improving the capacity of the Bostrom-Felbinger protocol [J]. *Physical Review A*, 2004, **69**: 054301.

[5] WANG C, DENG F G, LONG G L. Multi-step quantum secure direct communication using multi-particle Green-Horne-Zeilinger state[J]. *Optics Communications*, 2005, **253**(1-3): 15-20.

[6] YAN X, SONG H S. Controlled quantum secure direct communication using a non-symmetric quantum channel with quantum superdense coding[J]. *Physics Letters A*, 2007, **364**(2): 117-122.

[7] LIN S, WEN Q Y, GAO F, *et al*. Quantum secure direct communication with $\chi$-type entangled states [J]. *Physical Review A*, 2008, **78**: 064304.

[8] CHEN X B, WANG T Y, DU J Z, *et al*. Controlled quantum secure direct communication with quantum encryption [J]. *International Journal of Quantum Information*, 2008, **6**(3): 543-551.

[9] CHEN X B, WEN Q Y, GUO F Z, *et al*. Controlled quantum

secure direct communication with W state[J]. *International Journal of Quantum Information*, 2008, **6**(4): 899-906.

[10] HUANG W, WEN Q Y, JIA H Y, *et al*. Fault tolerant quantum secure direct communication with quantum encryption against collective noise[J]. *Chinese Physics B*, 2012, **21**(10): 100308.

[11] ZHANG Z J, MAN Z X. Secure direct bidirectional communication protocol using the Einstein-Podolsky-Rosen pair block[DB/OL]. [2013-06-13]. http://arxiv.org/pdf/quant-ph/0403215.pdf.

[12] ZHANG Z J, MAN Z X. Secure bidirectional quantum communication protocol without quantum channel[DB/OL]. [2013-06-13]. http://arxiv.org/pdf/quant-ph/0403217.pdf.

[13] ZHANG Z J, MAN Z X, LI Y. Economically improving message-unilaterally-transmitted quantum secure direct communication to realize two-way communication[DB/OL]. [2013-06-13]. http://arxiv.org/pdf/quant-ph/0406181.pdf.

[14] NGUYEN B A. Quantum dialogue[J]. *Physics Letters A*, 2004, **328**(1): 6-10.

[15] MAN Z X, ZHANG Z J, LI Y. Quantum dialogue revisited [J]. *Chinese Physics Letters*, 2005, **22**(1): 22-24.

[16] JIN X R, JI X, ZHANG Y Q, *et al*. Three-party quantum secure direct communication based on GHZ states[J]. *Physics Letters A*, 2006, **354**(1-2): 67-70.

[17] MAN Z X, XIA Y J. Controlled bidirectional quantum direct communication by using a GHZ state[J]. *Chinese Physics Letters*, 2006, **23**(7): 1680-1682.

[18] MAN Z X, XIA Y J, NGUYEN B A. Quantum secure direct communication by using GHZ states and entanglement swapping[J]. *Journal of Physics B*, 2006, **39**: 3855-3863.

[19] MAN Z X, XIA Y J. Improvement of security of three-party quantum secure direct communication based on GHZ states [J]. *Chinese Physics Letters*, 2007, **24**(1): 15-18.

[20] CHEN Y, MAN Z X, XIA Y J. Quantum bidirectional secure direct communication via entanglement swapping[J]. *Chinese Physics Letters*, 2007, **24**(1): 19-22.

[21] YANG Y G, WEN Q Y. Quasi-secure quantum dialogue using single photons[J]. *Science in China Series G*, 2007, **50**(5): 558-562.

[22] GAO F, QIN S J, WEN Q Y, *et al*. Comment on: Three-party quantum secure direct communication based on GHZ states[J]. *Physics Letters A*, 2008, **372**(18): 3333-3336.

[23] GAO F, GUO F Z, WEN Q Y, *et al*. Revisiting the security of quantum dialogue and bidirectional quantum secure direct communication[J]. *Science in China Series G*, 2008, **51**(5): 559-566.

[24] SHAN C J, LIU J B, CHENG W W, *et al*. Bidirectional quantum secure direct communication in driven cavity QED [J]. *Modern Physics Letters B*, 2009, **23**(27): 3225-3234.

[25] YE T Y, JIANG L Z. Improvement of controlled bidirectional quantum direct communication using a GHZ state[J]. *Chinese Physics Letters*, 2013, **30**(4): 040305.

[26] LIU Z H, CHEN H W. Comment on "Improvement of controlled bidirectional quantum direct communication using a GHZ state"[J]. *Chinese Physics Letters*, 2013, **30**(7): 079901.

[27] YE T Y, JIANG L Z. Reply to the comment on "Improvement of controlled bidirectional quantum direct communication using a GHZ state"[J]. *Chinese Physics Letters*, 2013, **30**(7): 079902.

[28] SHI G F, XI X Q, TIAN X L, *et al*. Bidirectional quantum secure communication based on a shared private Bell state[J]. *Optics Communications*, 2009, **282**(12): 2460-2463.

[29] SHI G F, XI X Q, HU M L, *et al*. Quantum secure dialogue by using single photons[J]. *Optics Communications*, 2010, **283**(9): 1984-1986.

[30] SHI G F. Bidirectional quantum secure communication scheme based on Bell states and auxiliary particles[J]. *Optics Communications*, 2010, **283**(24): 5275-5278.

[31] GAO G. Two quantum dialogue protocols without information leakage[J]. *Optics Communications*, 2010, **283**(10): 2288-2293.

[32] YE T Y, JIANG L Z. Information leakage prevention in quantum dialogue using the measurement correlation after entanglement swapping and decreasing the transmission efficiency[J]. *Acta Photonica Sinica*, 2013, **42**(11): 1311-1318.

[33] SHAN C J, LIU J B, CHEN T, *et al*. Controlled quantum secure direct communication with local separate measurements in cavity QED[J]. *International Journal of Theoretical Physics*, 2010, **49**: 334-342.

[34] ZHENG S B. Generation of entangled states for many multilevel atoms in a thermal cavity and ions in thermal motion[J]. *Physical Review A*, 2003, **68**: 035801.

[35] ZHENG S B, GUO G C. Efficient scheme for two-atom entanglement and quantum information processing in cavity QED[J]. *Physical Review Letters*, 2000, **85**(11): 2392-2395.