Computers, Materials & Continua CMC, vol.64, no.2, pp.1247-1260, 2020

A Controlled Quantum Dialogue Protocol Based on Quantum Walks

Jinqiao Dai[1], Shibin Zhang[1, *], Yan Chang[1], Xueyang Li[1], Tao Zheng[1] and Jinyue Xia[2]

Abstract: In order to enable two parties to exchange their secret information equally, we propose a controlled quantum dialogue protocol based on quantum walks, which implements the equal exchange of secret information between the two parties with the help of the controller TP. The secret information is transmitted via quantum walks, by using this method, the previously required entangled particles do not need to be prepared in the initial phase, and the entangled particles can be produced spontaneously via quantum walks. Furthermore, to resist TP's dishonest behavior, we use a hash function to verify the correctness of the secret information. The protocol analysis shows that it is safe and reliable facing some attacks, including intercept-measure-resend attack, entanglement attack, dishonest controller's attack and participant attack. And has a slightly increasing efficiency comparing with the previous protocols. Note that the proposed protocol may be feasible because quantum walks prove to be implemented in different physical systems and experiments.

Keywords: Quantum cryptography, controlled quantum dialogue, quantum walks, quantum teleportation.

1 Introduction

Since Shannon [Shannon (1948)] published "Communication Theory of Secret Systems", cryptography has become the fundamental subject in the study of information security. As we all know the classic cryptography protocols are based on some difficult math problems. However, with the development of quantum technology and the realization of quantum computers, classical cryptosystems might be in potential danger. To conquer these problems, researchers put effort into quantum cryptography, and soon the first quantum cryptography protocol BB84 [Bennett (1984)] is proposed. The BB84 protocol is used to distribute quantum keys. From then on, quantum cryptography has attracted lots of attention and established many interesting branches, such as quantum key distribution QKD [Cabello (2000); Zhang and Song (2014); Liu, Gao, Li et al. (2018); Jin, Bourgoln, Tannous et al. (2019)], quantum secure direct communication (QSDC)

[1] Chengdu University of Information Technology, Chengdu, 610225, China.

[2] International Business Machines Corporation (IBM), New York, 10421, USA.

[*] Corresponding Author: Shibin Zhang. Email: cuitzsb@cuit.edu.cn.

Received: 09 March 2020; Accepted: 17 April 2020.

[Gu, Huang, Fang et al. (2011); Liu, Cheng and Jiang (2012); Cao, Li and Peng (2018); He, Ma and Wu (2019); Yang and Tsal (2020)], quantum secrets haring (QSS) [Hao, Li and Long (2010); Hao, Wang and Long (2011); Liu, Xu, Zhang et al. (2019)], quantum private comparison [Yan, Zhang and Chang (2019)], etc.

Different from QKD, quantum secure direct communication (QSDC) is a distinct protocol, which allows two legitimate users to transmit their secret information directly in a secure way without sharing a key to encrypt it beforehand. Thereby, QSDC protocols have a high-security demand for the communication channel, and it is very useful and important especially in urgent conditions. Thus, many protocols based on QSDC have been presented [Chang, Xu and Zhang (2014); Chang (2015)]. QSDC protocols permit one-way communication between the users, while bidirectional quantum direct communication allows two users to exchange their secret information simultaneously, the so-called quantum dialogue (QD). In 2004, Nguyen [Nguyen (2004)] outlined the first quantum dialogue protocol. In 2005, Gao et al. [Gao, Yan and Wang (2005)] introduced a controller into the design of QD for the first time in which the users employ a controller to supervise the communication. There are two requirements a secure CQD protocol [Kao and Hwang (2016)] should be satisfied: the users cannot obtain secret information from the others without the help of the controller and the controller cannot obtain the secret information. Since the CQD protocol proposed, many other similar and improved protocols have also been proposed. In 2007, Xia et al. [Xia, Man and Wang (2007)] proposed a controlled secure quantum dialogue protocol by taking advantage of a pure entangled GHZ state. In 2013, Ye et al. [Ye and Jiang (2013)] pointed out that there exists the information problem in Xia et al.'s [Xia, Man and Wang (2007)] protocol and gave two improved schemes based on GHZ states and Bell states to avoid the problem. In 2015, Chang [Chang (2015)] showed that Ye et al.'s [Ye and Jiang (2013)] protocol is assailable to an intercept-and-resend attack and provided an improved protocol via applying Bell states. Then, in 2017, Kao et al. [Kao and Hwang (2017)] proposed a new CQD protocol by taking advantage of the four-particle cluster entangled states which are robust against most attacks and has a higher efficiency, but without considering the case that the controller is unfaithful. And in 2018, Qi et al. [Qi, Gang and Cai (2018)] proposed a two authenticated quantum dialogue protocols using three-particle entangled states. Also, many other studies have provided many novel ideas for the development of quantum encryption [Wu and Yang (2019)].

Quite recently, quantum walk (QW) has been employed for realizing quantum teleportation [Wang, Shang and Xue (2017); Shang, Wang and Li (2018)]. Compared with the existing teleportation protocols, QW-based teleportation shows interesting properties. For example, prior entangled states are not needed anymore (It is viewed as an improvement in terms of the generation of the required entangled states) and the essential entanglement resource is produced spontaneously via the QW. The concept of the quantum walk was firstly introduced by Aharonov et al. [Aharonov, Davidovich and Zagury (1993)]. Then the model of on the line was proposed by Ambainis et al. [Ambainis, Bachy, Nayakz et al. (2001)] and it was developed on the graphs by Aharonov et al. [Aharonov, Ambainis, Kempe et al. (2001)]. QW can be classified into discrete-time QW (DTQW) [Meyer (1996)] and continuous-time QW (CTQW) [Farhi and Gutmann (1998); Shikano (2013)]. The relationship between DTQW and CTQW has

also been established [Childs (2010)]. On the one hand, QW has proven to be a promising resource in quantum information processing tasks and has potential in designing algorithms [Potoˇcek, Gbris, Kiss et al. (2009)]. On the other hand, the implementation of QW has been made in different physical systems [Di, Hillery and Zubairy (2004); Eckert, Mompart and Birkl (2005)], and experimental implementations [Bian, Li, Zhan et al. (2017); Tang, Lin, Feng et al. (2018)] have also been reported. Therefore, it is necessary and useful to discuss the application of quantum walks in CDQ protocols.

Through the above analysis, we realize that most of the previous CDQ protocols lack discussion of the dishonest controller's attack. Besides, the particle states they prepared in the first place were most GHZ states and multi-particle cluster states which cannot be easily implemented with the existing technology. To solve these issues, we proposed a CDQ protocol based on quantum walks which shows higher efficiency and can defend against most attacks including intercept-measure-resend attack, entanglement attack and dishonest controller's attack. Moreover, by using quantum walks to teleport unknown qubit make the prior entangled states are not needed anymore, the entangled states are produced spontaneously during the steps of quantum walks.

The rest of this paper is outlined as follows. In Section 2, we briefly introduce the theory of quantum walks to teleport unknown qubits which will be used in the next section. And then in Section 3, we proposed the CQD protocols based on quantum walks. Then, we analyze the security and efficiency of the proposed protocol in Section 4. And the conclusion is drawn in Section 5.

2 Preliminary theory

2.1 Quantum walks on the line

In this protocol, we use quantum walks to teleport an unknown qubit. Before giving our specific steps of the protocol, the theory of quantum walks and some related knowledge need to be reviewed [Wang, Shang and Xue (2017)].

Quantum walks use a compound Hilbert space including two different spaces, including position space and coin space, where the position space defined as $H_p = \{|n\rangle, n \in Z\}$ and the coin space defined as $H_c = \{|0\rangle, |1\rangle\}$. Thus, the compound Hilbert space can be expressed as $H = H_p \otimes H_c$. And each step of quantum walks can be described as a series of equations.

$$W^{(l)} = E^{(l)} \cdot (I \otimes C) \tag{1}$$

$$E = S \otimes |0\rangle\langle 0| + S^{\dagger} \otimes |1\rangle\langle 1| \tag{2}$$

$$S = \sum\nolimits_n |n+1\rangle\langle n| \tag{3}$$

In the above equations, C means the coin operator action on coin space, any qubit operations can be chosen to fulfill the quantum walks and I is the operated particle. S is the shift operator, and the Eq. (2) simulates the classical way of random walks. In the process of quantum walks, if the measurement of coin space is $|0\rangle$, the walker steps

forwards from $|n\rangle$ to $|n+1\rangle$ and if the measurement of coin space is $|1\rangle$, the walker steps backward to $|n-1\rangle$.

2.2 Teleport a qubit by quantum walks

Assume that the sender Alice wants to transmit an unknown qubit $|\Psi\rangle=\cos\theta|0\rangle+\sin\theta|1\rangle$ to the receiver Bob, where the plural satisfies the principle of normalization $|\cos\theta|^2+|\sin\theta|^2=1$. In order to complete the teleportation, Alice needs to prepare two particles, one of the particles contains the state of the unknown qubit called A1 which can also be denoted as coin1, and the other one contains the state of the position space called Pa. Meanwhile, Bob prepares particle A2 denoted as coin2. The state of particle Pa and A2 are both $|0\rangle$.

The teleportation requires two steps, the first step of quantum walks can be described as:

$$W^{(1)}=E^{(1)}\cdot(I_p\otimes C_1\otimes I_1) \tag{4}$$

$$E=S\otimes|0\rangle_1\langle 0|\otimes I_2+S^{\dagger}\otimes|1\rangle_1\langle 1|\otimes I_2 \tag{5}$$

In Eqs. (4) and (5), I_p is the state of position space and I_1 is the state of coin1, C_1 is the operation acting on coin1, we choose C_1=I as a quantum operation example. And the second step of quantum walks can be described as.

$$W^{(2)}=E^{(2)}\cdot(I_p\otimes H\otimes I_2) \tag{6}$$

$$E=S\otimes|0\rangle_2\langle 0|\otimes I_1+S^{\dagger}\otimes|1\rangle_2\langle 1|\otimes I_1 \tag{7}$$

In Eqs. (6) and (7), H means the Hadamard operation acting on coin2. The other symbols have the same meaning as Eqs. (4) and (5). It is worth noting that H can be replaced by I if the state of coin2 is $|+\rangle$. Then Alice measures particle A1 with Z basis $\{|+\rangle,|-\rangle\}$ and records the measurement results β1 ($|+\rangle$ as 1, $|-\rangle$ as -1). After that, Alice measures Pa with a prepared basis $|L\rangle=\{|-2'\rangle,|-1\rangle,|0\rangle,|1\rangle,|2'\rangle\}$, where $|\pm 2'\rangle=(|-2\rangle\pm|2\rangle)/\sqrt{2}$, and records the measurement results β2 as -1, 0, 1 corresponding to $|-2'\rangle,|0\rangle,|2'\rangle$ in the measurement results, then Alice sends the measurement results to Bob. After Bob receives β1 and β2, he performs the corresponding Pauli operations on particle A2 to recover the unknown qubit $|\Psi\rangle$. The relationship between measurement results and Pauli operations is shown in Tab. 1.

Table 1: The relationship between measurement results and Pauli operations

Measurement results of A1 (β1)	Measurement results of Pa (β2)	Pauli operations
1/-1	1/-1	I
1/-1	-1/1	Z
1	0	X
-1	0	ZX

3 The proposed protocol

3.1 Alice sends information to Bob via quantum walks

Step 1. Alice prepares n qubits particles A1 according to her secret information Ma=(ma (1), ma (2), …, ma (n)). For uniformity, all transmitted quantum states A1 are assumed to be in the state $\cos\theta|0\rangle+\sin\theta|1\rangle$, where $|\cos\theta|^2+|\sin\theta|^2=1$. Then Alice prepares n qubits position particles Pa, the initial state of Pa is $|0\rangle$. After that, Alice informs TP to prepare n qubits particles A2, the initial state of A2 is also $|0\rangle$. Therefore, the initial state of the teleportation system can be described as follows.

$$|\Phi\rangle=|0\rangle_p\otimes(\cos\theta|0\rangle+\sin\theta|1\rangle)_1\otimes|0\rangle_2 \tag{8}$$

Step 2. Alice firstly uses particles A1 as coin space and particles Pa as the position space to perform the first step of quantum walks Wa. Which can be described as follows.

$$W_a^{(1)}=E^{(1)}\cdot(I_p\otimes C_1\otimes I_1) \tag{9}$$

And after the first step of Wa, the entire state of the system is transformed into

$$W_a^{(1)}=\left(\cos\theta|100\rangle+\sin\theta|-110\rangle\right)_{p12} \tag{10}$$

It can be seen from Eq. (10), particles A1 and Pa have been entangled. After that Alice randomly chooses k qubits from particles A1 as decoy particles. Here, the decoy particles are denoted as A1' and the corresponding entangled particles are denoted as Pa'. Then she randomly inserts particles Al' into the rest particles Pa and sends them to TP. Particles A1 and Pa' are retained by herself. Note that only Alice knows the specific position of A1' and the block transmission technology is used to send Pa and A1' [Liu, Cheng and Jiang (2012)].

Step 3. After receiving particles Pa and A1' from Alice, TP informs Alice to initiate eavesdropping detection. Alice measures particles Pa' with $|L\rangle$ basis, then announces the measurement results and the position of the decoy particles A1'. After that TP uses Z basis to measure particles A1'. The measurement results of particles A1' and Pa' should satisfy the relationship of Tab. 2. Then TP calculates the corresponding error rate according to Tab. 2. If the total error rate is lower than the threshold, TP will continue the communication and proceed to the next step. Otherwise, the communication will be terminated.

Table 2: the relationship between particles A1'/B1' and Pa'/Pb'

The measurement results of A1'/B1' ($\|L\rangle$ basis)	The measurement results of Pa'/Pb' (Z basis)
$\|1\rangle$	$\|0\rangle$
$\|-1\rangle$	$\|1\rangle$

Step 4. TP uses the prepared particles A2 as a new coin space and Pa as position space to initiate the second step of Wa. And the entire state of the system is transformed into

$$W^{(2)}=\left(\cos\theta|200\rangle+\cos\theta|001\rangle+\sin\theta|010\rangle+\sin\theta|-211\rangle\right)_{p12} \tag{11}$$

Then TP sends particles A2 to Bob.

Step 5. After Bob receives particles A2 from TP, he informs Alice to measure particles A1 with X basis $\{|+\rangle,|-\rangle\}$ and record the measurement results ($|+\rangle$ as 1, $|-\rangle$ as -1), the measurement results are denoted as α_1, then Alice sends α_1 to Bob. After that, Bob prepares to send his secret information to Alice. At this moment, Bob cannot recover the complete information of Alice until TP publishing the corresponding information. This corresponding information will be mentioned in the verification phase.

3.2 Bob sends information to Alice via quantum walks

Step 6. Bob prepares n qubits particles B1 according to his secret information Mb=(mb (1), mb (2), …, mb (n)), Then he prepares n qubits position particles Pb and informs TP to prepare n qubits particles B2. The preparing step of Bob and TP are the same as Step 1. This means the initial state of B2 and Pb are both $|0\rangle$ and the initial state of the teleportation system is the same as Eq. (8). The following steps of Bob sending information to Alice are the same as Steps 2 to 5.

Step 7. Bob firstly uses particles B1 as coin space and particles Pb as position space to initiate the first step of quantum walks Wb and after the first step of Wb, the entire state of the system is transformed into

$$W_b^{(1)} = \left(\cos\theta\,|100\rangle + \sin\theta\,|-110\rangle\right)_{p12} \tag{12}$$

Then Bob chooses the decoy particles in the same way as Alice, the decoy particles B1 denoted as B1' and the corresponding entangled particles Pb are denoted as Pb'. Then Bob uses block transmission technology to send particles Pb and B1' to TP and only he knows the specific position of B1.

Step 8. After receiving particles Pb and B1' from Bob, TP informs Bob to initiate the same eavesdropping detection as Alice did in Step 3. Therefore, the measurement results of particles B1' and Pb' should satisfy the relationship of Tab. 2. Then TP calculates the corresponding error rate according to Tab. 2. If the total error rate is lower than the threshold, TP will continue the communication and proceed to the next step. Otherwise, the communication will be terminated.

Step 9. TP uses the prepared particles B2 as a new coin space and Pb as position space to initiate the second step of Wb. Then TP sends particles B2 to Alice. The entire state of the system is transformed into

$$W_b^{(2)} = \left(\cos\theta\,|200\rangle + \cos\theta\,|001\rangle + \sin\theta\,|010\rangle + \sin\theta\,|-211\rangle\right)_{p12} \tag{13}$$

Step 10. After Alice receives particles B2 from TP, he informs Bob to measure particles B1 with X basis and records the measurement results as β_1, then Bob sends the measurement results β_1 to Alice. After both Alice and Bob receive their measurement results, they inform TP to perform the verification phase.

3.3 Verification phase

Step 11. TP measures particles Pa and Pb with $|L\rangle$ basis, the measurement results are denoted as α_2 and β_2 and he announces α_2 and β_2. Then Alice and Bob can select the corresponding Pauli operations based on the measurement results announced by the other party and TP. The relationship between the measurement results and the Pauli operation is shown in Tab. 1. Then Alice and Bob perform corresponding Pauli operations on particles A2 and B2 to recover the state of particles B1 and A1, respectively. Thus, they can both obtain the secret information of the other party. The obtained secret information is denoted as Ma' and Mb'.

Step 12. To verify the accuracy of the secret information, Alice adds Ma and Mb' bitwise, and inputs it into a hash function, the result of the hash function called S1. Meanwhile, Bob uses the same method to adds Mb and Ma' bitwise and gets the result of the hash function, called S2. Then Alice and Bob announce S1 and S2. If S1=S2, Alice and Bob successfully obtain each other's secret information, otherwise the measurement results announced by TP are incorrect.

4 Protocol analysis

4.1 Intercept-measure-resend attack

Assuming an external eavesdropper Eve wants to eavesdrop on Alice's secret information. He has to intercept all the particles Alice send to TP in Step 2 and measure them with an appropriate measurement basis. Since Eve doesn't know the specific position of decoy particles, for each particle he has to choose to measure it with Z basis or $|L\rangle$ basis. If Eve uses $|L\rangle$ basis to measure A1', the state of A1' will collapse into $|-1\rangle, |0\rangle$ or $|1\rangle$ and this kind of disturbing will be easily detected in Step 3. The possibility of choosing the correct measurement basis is 1/2. For k qubits particles A1', the total possibility of passing the eavesdropping detection is $1/2^k$, if the value of k is appropriate, it is likely to detect Eve's Intercept-measure-resend attack.

However, since k is used to determine the number of decoy particles, it means that the value of k should not exceed half of the total number of n. Therefore, it is still possible for Eve to pass eavesdropping detection. Suppose Eve has passed the eavesdropping detection. He has to measure Pa with $|L\rangle$ basis to obtain the complete information of Pa. Since Eve still does not know the exact position of Pa, he has to measure them with Z basis or $|L\rangle$ basis like decoy particles. And the possibility of Eve successfully obtaining Alice's complete information depends on the binomial distribution. Assume that m represents the number of qubits being measured with the correct measurement basis, for n qubits particles, the possibility of obtaining Alice's complete information can be defined as follows.

$$P = \binom{n}{m}\left(\frac{1}{2}\right)^m \left(\frac{1}{2}\right)^{n-m} \tag{14}$$

The Binomial coefficient can be defined as:

$$\binom{n}{m}=\frac{n!}{m!(n-m)!} \tag{15}$$

Thus, the graph of P is shown in Fig. 1.

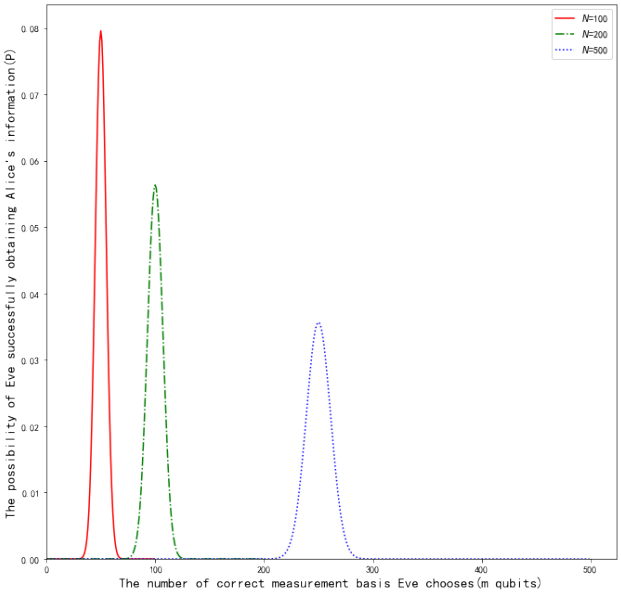

Figure 1: The possibility of Eve successfully obtaining Alice's information

It can be seen from Eq. (14) and Fig. 1. The possibility of obtaining Alice's complete information depending on m and n. According to the characteristics of the binomial distribution, when n is different, P always has a maximum value. Moreover, the peak value of P decreases as n increases. It can be deduced that P will be quite small when n is large enough. In summary, Eve cannot obtain Alice's information through this attack.

4.2 Entanglement attack

Assuming that Eve attempts to eavesdrop on Alice's secret information. Since he does not know which particles are used to detect eavesdropping, he has to perform the same attack on all intercepted particles and send them back to the TP. For decoy particles A1', after performing the attack operation $\hat{E}$, the state of the composite system of Alice, TP and Eve is

$$|\varphi\rangle = \sum_{a,t\in\{0,1\}} |\varepsilon_{a,t}\rangle |a\rangle |t\rangle \tag{16}$$

where $|\varepsilon_{a,t}\rangle$ denotes Eve's probe state, $|a\rangle$ and $|t\rangle$ are single-particle states of Alice and TP in each entangled states, respectively. The condition on the state of Eve's probe particle is

$$\sum_{a,t\in\{0,1\}} \langle\varepsilon_{a,t}|\varepsilon_{a,t}\rangle = 1 \tag{17}$$

After the decoy particles attacked by Eve, the states $|0\rangle$ and $|1\rangle$ become

$$|\varphi'_0\rangle = \hat{E}|0,\varepsilon\rangle = a|0,\varepsilon_{00}\rangle + b|1,\varepsilon_{01}\rangle \tag{18}$$

$$|\varphi'_1\rangle = \hat{E}|1,\varepsilon\rangle = c|0,\varepsilon_{10}\rangle + d|1,\varepsilon_{11}\rangle \tag{19}$$

where $|a|^2 + |b|^2 = 1$, $|c|^2 + |d|^2 = 1$, $|a|^2 = |d|^2 = F$, $|b|^2 + |c|^2 = D$.

Suppose after the first step of Wa, Alice sends k qubits A1' to Bob. After attack operator Ê is performed, the state of the composed system becomes

$$|\varphi\rangle_{Eve} = \cos\theta\left[|1\rangle_A(a|0,\varepsilon_{00}\rangle + b|1,\varepsilon_{01}\rangle)_{TE}\right] + \sin\theta\left[|-1\rangle_A(c|0,\varepsilon_{10}\rangle + d|1,\varepsilon_{11}\rangle)_{TE}\right] \tag{20}$$

where subscript A represents particles held by Alice, subscript T represents particles held by TP and subscript E represents the probe particles. It can be seen from Eq. (20) that the decoy particles are entangled with the probe particles. To show the relationship between the entangled particles more intuitively, we take the θ angle as 45 degrees. In this case, the composed system becomes

$$\begin{aligned} |\varphi\rangle_{Eve} &= \frac{1}{\sqrt{2}}\left((a|1,0,\varepsilon_{00}\rangle + b|1,1,\varepsilon_{01}\rangle + (c|-1,0,\varepsilon_{10}\rangle + d|-1,1,\varepsilon_{11}\rangle)\right)_{ATE} \\ &= \frac{1}{\sqrt{2}}\left[(a|1,\varepsilon_{00}\rangle + c|-1,\varepsilon_{10}\rangle)_{AE}|0\rangle_T + (b|1,\varepsilon_{01}\rangle + d|-1,\varepsilon_{11}\rangle)_{AE}|1\rangle_T\right] \end{aligned} \tag{21}$$

During the eavesdropping detection, TP uses Z basis to measure particles A1', $|\varphi\rangle_{Eve}$ will collapse into $(a|1,\varepsilon_{00}\rangle + c|-1,\varepsilon_{10}\rangle)$ or $(b|1,\varepsilon_{01}\rangle + d|-1,\varepsilon_{11}\rangle)$ with the possibility of 1/2. No matter what kind of state $|\varphi\rangle_{Eve}$ collapses into, the state of Pa' has been changed and will be detected by Alice and TP. It means that if Eve attacks particles in an entangled state, the eavesdropper's interference will inevitably introduce errors so that the presence of the eavesdropper can be detected with a possibility of:

$$P_d = |b|^2 = 1 - |a|^2 = |c|^2 = 1 - |d|^2 \tag{22}$$

When Eve does not want to be detected, the probe particles must be directly related to particles A1'. However, there is no correlation between them, thus Eve cannot get any useful information, which proves that the entanglement attack strategy will not be successful.

4.3 Dishonest controller's attack

Assume that the controller TP is not honest and reliable, he expects that Alice and Bob are unable to complete the dialogue of secret information. TP implements fake signal attack, specifically, by announcing wrong measurement results after measuring Pa and Pb with $|L\rangle$ basis. In this case, Alice and Bob will get the wrong Ma' and Mb' based on the wrong results. However, Alice and Bob will add the deduced Ma' and Mb' by bitwise with their secret information in the verification phase, then enter it as an input to hash function to get S1 and S2. And according to the value of S1 and S2, Alice and Bob can judge whether TP uses a fake signal attack. Therefore, the protocol can resist this attack. On the other hand, if TP attempts to obtain users' secret information, he has to perform corresponding Pauli operations on particles A2 and B2. Thus, he will keep particles A2 and B2 and prepare fake particles to Alice and Bob, in this way he can obtain users'

secret information. However, this kind of attack is the same as a fake signal attack, which will be easily detected during the verification of users' hash values. Thus, the attack of the dishonest controller cannot be successful.

4.4 Participant attack

Assume that Bob wants to deceive Alice during the communication process, that is, instead of preparing particle states according to his secret information Mb, he randomly prepares a series of particle states and sends them to TP. In this case, TP cannot detect this kind of attack. But when TP announces measurement results to Alice, Alice's deduced secret information is different from Mb, denoted as Mb', so Alice's hash result and Bob's hash result will be different. At this time, Alice finds someone had performed the deception attack during the communication process. On the other hand, if Bob attempts to intercept Alice's particles to illegally obtain Alice's secret information. In this case, Bob was considered as an external eavesdropper Eve, as discussed in Sections 4.1 and 4.2, no matter which attack strategy Bob adopts, this attack strategy will never work.

4.5 Efficiency analysis

To analysis the efficiency of the proposed protocol, we compare the proposed protocol with some previous protocols. The performance of quantum protocols can be characterized by qubit efficiency [Cabello (2000)] which is defined as

$$\eta = \frac{b_s}{q_t + b_t} \tag{23}$$

where b_s is the total number of transmitted classical bits, q_t is the total number of qubits utilized in the protocol, and b_t expresses the number of classical bits utilized to decode the information.

In our proposed protocol, Alice prepares 2n qubits particles and sends n qubits particles to TP. After that TP prepares another n qubits particles as new coin space and sends n qubits particles to Bob. To receive Alice's secret information, Bob needs Alice and TP to measure their particles A1 and Pa and announce their measurement results in the classic channel, the transmitted classical bits are 2n bits. Thus, the efficiency of our proposed protocol is $\eta = 2n/(3n+2n) = 40\%$, the efficiency comparison of the proposed protocol with the previous protocols are demonstrated in Tab. 3.

Table 3: Comparison of previous protocols and our CQD protocol

Protocol	η (%)	Quantum states the protocol prepares
Chang [Chang (2015)]	22	Bell states
Kao et al. [Kao and Hwang (2016)]	18	GHZ and Bell states
Kao et al. [Kao and Hwang (2017)]	20	Four-particle cluster states
Qi et al. [Qi, Gang and Cai (2018)]	25	Three-particle entangled states
Our CQD protocol	40	Single-particle states

It is explicit that the efficiency of our protocol is slightly higher than most of the previous protocols. Furthermore, the quantum states our protocol prepares are single-particle states, the entanglement particle states are produced spontaneously via quantum walks.

5 Conclusions

In this paper, we propose a controlled quantum dialogue protocol based on quantum walks. During the communication process, users exchange their secret information simultaneously using quantum walks, and they cannot obtain other's secret information without the help of TP. And to prevent the controller's dishonest behavior, users compare the hash value of their secret information. Comparing with recent CQD protocols, what our scheme optimized are as follows.

Firstly, we use quantum walks to teleport unknown qubits which allow users only need to prepare single-particle states in the intimal phase, the entangled states are produced spontaneously during the process of quantum walks. Besides, the protocol analysis shows that the protocol can resist intercept-measure-resend attack, entanglement attack, dishonest controller attack and participant attack. Finally, our protocol is more efficient than most previous protocols.

Funding Statement: This work is supported by the National Natural Science Foundation of China (Nos. 61572086 and 61402058), the Key Research and Development Project of Sichuan Province (Nos. 20ZDYF2324, 2019ZYD027 and 2018TJPT0012), the Innovation Team of Quantum Security Communication of Sichuan Province (No. 17TD0009), the Academic and Technical Leaders Training Funding Support Projects of Sichuan Province (No. 2016120080102643), the Application Foundation Project of Sichuan Province (No. 2017JY0168), the Science and Technology Support Project of Sichuan Province (Nos. 2018GZ0204 and 2016FZ0112).

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

Aharonov, Y.; Ambainis, A.; Kempe, J.; Vazirani, U.; (2001): Quantum walks on graphs. *Proceedings of the Thirty-Third Annual ACM Symposium on Theory of Computing*, pp. 50-59.

Aharonov, Y.; Davidovich, L.; Zagury, N. (1993): Quantum random walks. *Physical Review A*, vol. 48, no. 2, pp. 1687.

Ambainis, A.; Bachy, E.; Nayakz, A.; Vishwanathx, A.; Watrous, J.; (2001): One-dimensional quantum walks. *Proceedings of the Thirty-Third Annual ACM Symposium on Theory of Computing*, pp. 37-49.

Bennett, C. H. (1984): Quantum cryptography public key distribution and coin tossing. *Theoretical Computer Science*, vol. 560, no. 1, pp. 7-11.

Bian, Z. H.; Li, J.; Zhan, X.; Twamley, J. (2017): Experimental implementation of a quantum walk on a circle with single photons. *Physical Review A*, vol. 95, no. 5, pp. 052338.

Cabello, A. (2000): Quantum key distribution in the Holevo limit. *Physical Review Letters*, vol. 85, no. 26, pp. 5635-5638.

Cao, Z. W.; Li, Y.; Peng, J. Y. (2018): Controlled quantum secure direct communication protocol based on huffman compression coding. *International Journal of Theoretical Physics*, vol. 57, no. 12, pp. 3632-3642.

Chang, C. H. (2015): Intercept-and-resend attack on controlled bidirectional quantum direct communication and its improvement. *Quantum Information Processing*, vol. 14, no. 9, pp. 3515-3522.

Chang, Y.; Xu, C. X.; Zhang, S. B. (2014): Controlled quantum secure direct communication and authentication protocol based on five-particle cluster state and quantum one-time pad. *Chinese Science Bulletin*, vol. 59, no. 21, pp. 2541-2546.

Childs, A. M. (2010): On the relationship between continuous-and discrete-time quantum walk. *Communications in Mathematical Physics*, vol. 294, no. 2, pp. 581-603.

Di, T.; Hillery, M.; Zubairy, M. S. (2004): Cavity QED-based quantum walk. *Physical Review A*, vol. 70, no. 3, pp. 032304.

Eckert, K.; Mompart, J.; Birkl, G. (2005): One- and two-dimensional quantum walks in arrays of optical traps. *Physical Review A*, vol. 72, no. 1, pp. 012327.

Farhi, E.; Gutmann, S. (1998): Quantum computation and decision trees. *Physical Review A*, vol. 58, no. 2, pp. 915.

Gao, T.; Yan, F. L.; Wang, Z. X. (2005): Deterministic secure direct communication using GHZ states and swapping quantum entanglement. *Journal of Physics A: Mathematical and General*, vol. 38, no. 25, pp. 5761.

Gu, B.; Huang, Y. G.; Fang, X.; Zhang, C. Y. (2011): A two-step quantum secure direct communication protocol with hyper entanglement. *Chinese Physics B*, vol. 20, no. 10, pp. 100309.

Hao, L.; Li, J. L.; Long, G. L. (2010): Eavesdropping in a quantum secret sharing protocol based on Grover algorithm and its solution. *Science China (Physics, Mechanics & Astronomy)*, vol. 53, no. 3, pp. 491-495.

Hao, L.; Wang, C.; Long, G. L. (2011): Quantum secret sharing protocol with four state Grover algorithm and its proof-of-principle experimental demonstration. *Optics Communications*, vol. 284, no. 14, pp. 3639-3642.

He, R.; Ma, J. G.; Wu, J. W. (2019): A quantum secure direct communication protocol using entangled beam pairs. *Europhysics Letters*, vol. 127, no. 5, pp. 50006.

Jin, J.; Bourgoln, J. P.; Tannous, R.; Agne, S.; Pugh, C. J. et al. (2019): Genuine time-bin-encoded quantum key distribution over a turbulent depolarizing free-space channel. *Optics Express*, vol. 27, no. 26, pp. 37214-37223.

Kao, S. H.; Hwang, T. (2016): Controlled quantum dialogue robust against conspiring users. *Quantum Information Processing*, vol. 15, no. 10, pp. 4313-4324.

Kao, S. H.; Hwang, T. (2017): Controlled quantum dialogue using cluster states. *Quantum Information Processing*, vol. 16, no. 5, pp. 139.

Liu, D.; Cheng, J. L.; Jiang, W. (2012): High-capacity quantum secure direct communication with single photons in both polarization and spatial-mode degrees of freedom. *International Journal of Theoretical Physics*, vol. 51, no. 9, pp. 2923-2929.

Liu, P.; Gao, S. B.; Li, C. Y.; Guo, Q. (2018): High-efficiency quantum key distribution without key sifting. *Journal of the Optical Society of America B-Optical Physics*, vol. 35, no. 10, pp. 2608-2611.

Liu, W.; Xu, Y.; Zhang, M.; Chen, J.; Yang, C. (2019). A novel quantum visual secret sharing scheme. *IEEE Access*, vol. 7, no. 4, pp. 114374-114384.

Meyer, D. A. (1996): From quantum cellular automata to quantum lattice gases. *Journal of Statistical Physics*, vol. 85, no. 5, pp. 551-574.

Nguyen, B. A. (2004): Quantum dialogue. *Physical Review A*, vol. 328, no. 1, pp. 6-10.

Potoˇcek, V.; Gbris, A.; Kiss, T.; Jex, I. (2009): Optimized quantum random-walk search algorithms on the hypercube. *Physical Review A*, vol. 79, no. 1, pp. 012325.

Qi, J. M.; Gang, X.; Cai, X. B. (2018): Two authenticated quantum dialogue protocols based on three-particle entangled states. *Quantum Information Processing*, vol. 17, no. 9, pp. 247-266.

Shang, Y.; Wang, Y.; Li, M.; (2018): Quantum communication protocols by quantum walks with two coins. *Europhysics Letters*, vol. 124, no. 6, pp. 60009.

Shannon, C. E. (1948): Communication theory of secrecy systems. *The Bell System Technical journal*, vol. 28, no. 4, pp. 656-715.

Shikano, Y. (2013): From discrete time quantum walk to continuous time quantum walk in limit distribution. *Journal of Computational and Theoretical Nanoscience*, vol. 10, no. 7, pp. 1558-1570.

Tang, H.; Lin, X. F.; Feng, Z.; Chen, J. Y.; Sun, K. et al. (2018): Experimental two-dimensional quantum walk on a photonic chip. *Science Advances*, vol. 4, no. 5, pp. eaat3174.

Wang, Y.; Shang, Y.; Xue P.; (2017): Generalized teleportation by quantum walks. *Quantum Information Processing*, vol. 16, no. 9, pp. 221.

Wu, T. J.; Yang, Y. X. (2019): Detecting Android inter-app data leakage via compositional concolic walking. *Intelligent Automation and Soft Computing*, vol. 25, no. 4, pp. 755-766.

Xia, Y. J.; Man, Z. X.; Wang, Z. X. (2007): Controlled quantum n-party simultaneous direct communication. *Journal of Physics A: Mathematical and General*, vol. 48, no. 1, pp. 79.

Yan, L. L.; Zhang, S. B.; Chang, Y. (2019): Measure-resend semi-quantum private comparison scheme using GHZ class states. *Computers, Materials & Continua*, vol. 61, no. 2, pp. 877-887.

Yang, C. W.; Tsal, C. W. (2020): Advanced semi-quantum secure direct communication protocol based on bell states against flip attack. *Quantum Information Processing*, vol. 19, no. 4, pp. 126-138.

Ye, T. Y.; Jiang, L. Z. (2013): Improvement of controlled bidirectional quantum direct communication using a GHZ state. *Chinese Physics Letters*, vol. 30, no. 4, pp. 040305.

Zhang, C. M.; Song, X. T. (2014): Delayed error verification in quantum key distribution. *Chinese Science Bulletin*, vol. 59, no. 23, pp. 2825-2828.