Quantum Inf Process (2017) 16:147
DOI 10.1007/s11128-017-1598-7

# Controller-independent bidirectional quantum direct communication

**Amit Kumar Mohapatra**[1] · **S. Balakrishnan**[1]

Received: 19 April 2016 / Accepted: 8 April 2017


**Abstract** Recently, Chang et al. (Quantum Inf Process 14:3515–3522, 2015) proposed a controlled bidirectional quantum direct communication protocol using Bell states. In this work, the significance of Bell states, which are being used as initial states in Chang et al. protocol, is elucidated. The possibility of preparing initial state based on the secret message of the communicants is explored. In doing so, the controller-independent bidirectional quantum direct communication protocol has evolved naturally. It is shown that any communicant cannot read the secret message without knowing the initial states generated by the other communicant. Further, intercept-and-resend attack and information leakage can be avoided. The proposed protocol is like a conversion between two persons without the help of any third person with high-level security.

**Keywords** Quantum cryptography · Quantum dialogue · Controlled bidirectional quantum direct communication

## 1 Introduction

Since the ancient times, secret way of communication between the sender and the receiver is an essential task due to various reasons. In the recent years, quantum mechanics is being exploited for the purpose of secure communication, and hence, the subject of quantum cryptography has evolved naturally. In quantum cryptography,

✉ S. Balakrishnan
physicsbalki@gmail.com

Amit Kumar Mohapatra
omamit1199@gmail.com

[1] Department of Physics, School of Advanced Sciences, VIT University, Vellore 632014, India

Published online: 21 April 2017

generation and distribution of quantum key are extensively used for secure communication between the sender and the receiver. The first quantum key distribution (QKD) protocol is presented by Charles Bennett and Gilles Brassard in the year 1984 [1]. QKD aims at establishing an unconditional secure secret key between two authorized users. Differing from QKD, quantum direct communication (QDC) allows the users to communicate the secret messages directly without creating a key to encrypt them in advance. After the inception of Ping–Pong protocol by Bostrom and Felbinger [2] in 2002, the significance of QDC protocols is brought out by some of the studies [2–5]. While sharing of the quantum secure keys is a well-known concept in quantum key distribution, the method of sharing of secure direct communication among the $n$ number of parties is described in [5]. In this method, the secret message can be extracted by the receiver only if all the communicants collaborate. However, if one communicant is not genuine and he does not want them to communicate, then he will not announce his encrypted share, which will be a problem for the sender and receiver.

While QDC protocols permit one-way communication between the users, bidirectional QDC (BQDC) protocols allow two users to exchange their secret messages simultaneously. BQDC is introduced in the year 2004 by Nguyen [6]. In 2005, Man et al. [7] proposal resolves the problem of intercept-and-resend attack. Using Greenberger–Horne–Zeilinger (GHZ) states, BQDC protocol is proposed with the increase in the efficiency of information transmission [8]. It is to be mentioned that BQDC schemes with and without entanglement have been proposed [9–12]. Several security problems in BQDC protocols are pointed [13,14], and then, some schemes are proposed to overcome the drawbacks [15,16].

The exchange of secret messages between the users is achieved with a set of device under the supervision of a third party, and such a scheme is called controlled bidirectional quantum direct communication (CBQDC) protocol [17]. Such a protocol is proposed using GHZ states as well as Werner states [17–19]. To overcome information leakage problem in [17], CBQDC is proposed using a Bell state instead of GHZ state [20]. However, this protocol [20] still suffers from the information leakage problem and intercept-and-resend attack [21–23]. A user can obtain the other user's secret message without the controller's permission by performing the intercept-and-resend attack. In order to resolve this problem, Chang et al. [23] proposed an improvement by using four Bell states as the initial states of controller's resource, and it is shown that both intercept-and-resend attack and information leakage are solved. Quantum efficiency of a protocol captures the significance of quantum cryptographic protocol [24]. Hassanpour and Houshmand have proposed a controlled deterministic secure quantum communication protocol [25], where they have claimed the efficiency of their protocol is more compared to the other existing protocols. Later on, Anirban Pathak [26] has proposed a protocol, which is also generalized for unidirectional and bidirectional communication, and it is shown that the protocol is more efficient than Hassanpour and Houshmand protocol. Very recently, an efficient multiparty-controlled bidirectional quantum direct communication protocol is proposed [27].

The present work aims to find the optimal value of entanglement of quantum states necessary for the execution of Chang et al. protocol as the Bell states are the essential physical resource and difficult to implement. However, it is found that Bell states are necessary to run the protocol. Further, we present a protocol in which communicants

can share the secret messages without the help of the controller. In other words, we exhibit the case of bidirectional quantum direct communication without the influence of the controller. Thus, we propose a controller-independent bidirectional quantum direct communication. To indicate the significance of the proposed protocol, security analysis and qubit efficiency are discussed.

## 2 Chang et al. protocol

In this section, we brief the Chang et al. protocol [23], which is an improved version of Ye et al. [20]. The steps adopted in the protocol are given below, and the same is shown in Fig. 1.

*Step 1* Charlie prepares $(n + l + d)$ Bell states, where each state is in one of the four Bell states:

$$|\phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle_{AB}+|11\rangle_{AB}), \qquad |\phi^-\rangle = \frac{1}{\sqrt{2}}(|00\rangle_{AB}-|11\rangle_{AB}),$$
$$|\psi^+\rangle = \frac{1}{\sqrt{2}}(|01\rangle_{AB}+|10\rangle_{AB}) \quad \text{or} \quad |\psi^-\rangle = \frac{1}{\sqrt{2}}(|01\rangle_{AB}-|10\rangle_{AB}). \qquad (1)$$

$l$ and $d$ are the numbers for the first and second security checking, $n$ is the number of qubits which will be encoded as a secret message and $\frac{n}{2} = m_1 = m_2$ as suggested by Chang et al. The subscripts $A$ and $B$ denote the first and the second particles of each Bell state that belong to Alice and Bob, respectively. Now, Charlie will take the first particles of Bell states to form a sequence $A = \left[P_1(A), P_2(A), \ldots, P_{n+l+d}(A)\right]$ and the second particles to form a sequence $B = \left[P_1(B), P_2(B), \ldots, P_{n+l+d}(B)\right]$. He will send the sequence $A$ to Alice. For instance, $A_{(n+l+d)} = |\phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle+|11\rangle)]$ is the initial state prepared by Charlie, and the sequences are $A_n = |0\rangle, |1\rangle$ and $B_n = |0\rangle, |1\rangle$. Now, Charlie will send $A_n = |0\rangle, |1\rangle$ sequence to Alice.

*Step 2* Alice will send a confirmation to Charlie after receiving the sequence $A_n$. Alice will execute the first security checking with Charlie. If error rate goes beyond the threshold, they will abort the communication, else they will continue to the next step.

*Step 3* Charlie will send the sequence $B_n$ to Bob. Upon receiving the sequence $B_n$, Bob will send a confirmation to Charlie and Alice. Then, he will execute the second security checking with Alice.

*Step 4* If there is no eavesdropper, Alice and Bob will perform the unitary operations according to their secret messages on the sequences $A_n$ and $B_n$ to form the new sequences $A'_n$ and $B'_n$. Usually, two-bit secret messages $\{00, 01, 10, 11\}$ are encoded by the respective unitary operators $\{I, \sigma_z, \sigma_x, i\sigma_y\}$. For secure consideration, Alice and Bob will prepare a sufficient number of single particles $D$ in one of the four states $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$, where $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle+|1\rangle)$ and $|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle-|1\rangle)$. By inserting $D$ to the initial state $A'_n$ and $B'_n$, it will become $A'_D$ and $B'_D$, respectively. Alice and Bob then exchange the new states $A'_D$ and $B'_D$ with each other simultaneously and execute the security checking on $D$.

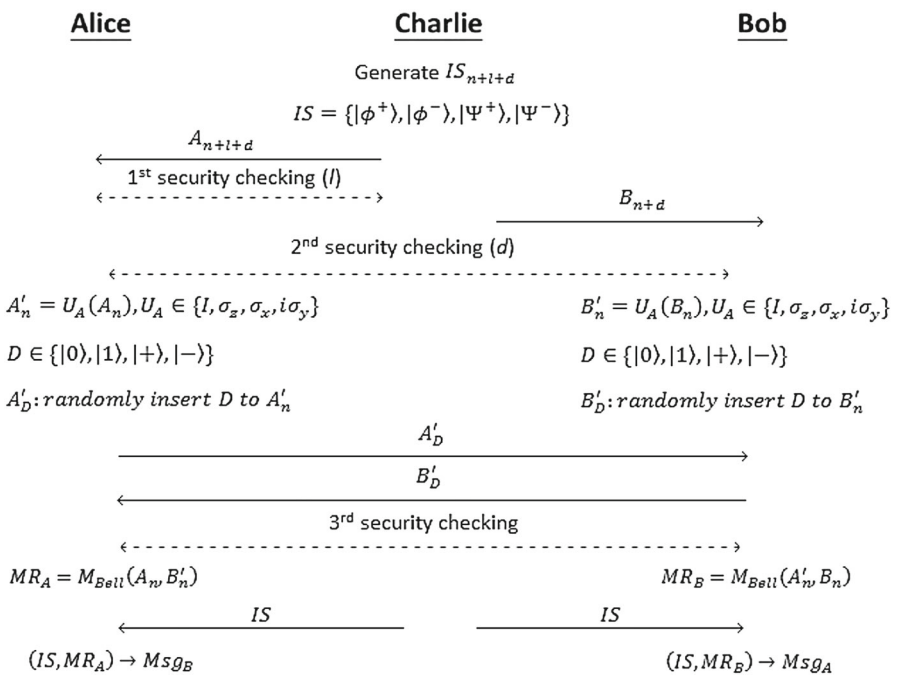


**Fig. 1** Chang et al. CBQDC protocol

**Table 1** Relation between Alice's (Bob's) measurements result $MR_A$ ($MR_B$), Charlie's initial states $IS$ and Bob's (Alice's) secret messages

| $MR_A$ | Bob's (Alice's) secret messages | | | |
|---|---|---|---|---|
| ($MR_B$) | 00 | 10 | 11 | 01 |
| Charlie's $IS$ | | | | |
| $\|\phi^+\rangle$ | $\|\phi^+\rangle$ | $\|\psi^+\rangle$ | $\|\psi^-\rangle$ | $\|\phi^-\rangle$ |
| $\|\psi^+\rangle$ | $\|\psi^+\rangle$ | $\|\phi^+\rangle$ | $\|\phi^-\rangle$ | $\|\psi^-\rangle$ |
| $\|\psi^-\rangle$ | $\|\psi^-\rangle$ | $\|\phi^-\rangle$ | $\|\phi^+\rangle$ | $\|\psi^+\rangle$ |
| $\|\phi^-\rangle$ | $\|\phi^-\rangle$ | $\|\psi^-\rangle$ | $\|\psi^+\rangle$ | $\|\phi^+\rangle$ |

Let Alice's secret message be 10 and Bob's secret message be 01, then, $Msg_A = |10\rangle \rightarrow \sigma_x$ and $Msg_B = |01\rangle \rightarrow \sigma_z$. After the unitary operation, the new sequences will be $A'_n = \sigma_x\ (|\ 0\rangle, |\ 1\rangle) = (|\ 1\rangle, |\ 0\rangle)$ and $B'_n = \sigma_z\ (|\ 0\rangle, |\ 1\rangle) = (|\ 0\rangle, -|\ 1\rangle)$.

*Step 5* Alice and Bob will perform a Bell measurement on the corresponding particles in sequences $B'_n$ and $A'_n$ and obtain the measurement result $MR_A$ and $MR_B$, respectively. If there is no eavesdropper, then Charlie will announce the initial state to let Alice and Bob communicate with each other. After getting the initial state and measurement results, Alice and Bob can deduce the secret messages according to Table 1.

By performing Bell measurement on $(A_n, B'_n)$, Alice will get $MR_A = |\phi^-\rangle$ and measurement on $(A'_n, B_n)$ will give $MR_B = |\Psi^+\rangle$ to Bob. After the announcement of initial state by Charlie, Alice will get the Bob's secret message $(IS, MR_A) \rightarrow Msg_B =$

$\left(|\phi^+\rangle, |\phi^-\rangle\right) \rightarrow |01\rangle$ and Bob will get Alice's secret message $(IS, MR_B) \rightarrow Msg_A = \left(|\phi^+\rangle, |\Psi^+\rangle\right) \rightarrow |10\rangle$.

As the four initial states, namely Bell states are being controlled by Charlie, the communicants cannot exchange their secret messages without knowing the initial state. Therefore, the intercept-and-resend attack is not possible for the malicious user, say Bob. Further, no information leakage is possible between Alice and Bob in the improved version of Ye et al. protocol [20].

## 3 Significance of initial states

In order to exhibit the significance of maximally entangled initial states, the following simple analysis is performed. Instead of four Bell states, we have introduced the following four arbitrary states as Charlie's initial state in the Chang et al. protocol:

$$\begin{aligned} |\omega^+\rangle &= \alpha|00\rangle + \beta|11\rangle, \quad |\omega^-\rangle = \alpha|00\rangle - \beta|11\rangle \\ |\chi^+\rangle &= \alpha|01\rangle + \beta|10\rangle, \quad |\chi^-\rangle = \alpha|01\rangle - \beta|10\rangle \end{aligned} \tag{2}$$

where $|\alpha|^2 + |\beta|^2 = 1$. Following the same steps of the Chang protocol as described in the preceding section, we have generated a new table indicating the relation between Alice's (Bob's) measurement result $MR_A$ ($MR_B$), Charlie's initial states $IS$ and Bob's (Alice's) secret messages (refer Table 2).

Even if the initial states are non-maximally entangled, Alice and Bob can communicate the secret message 00 or 01. However, the secret messages 10 and 11 cannot be communicated as the measurement results of Alice and Bob are not the same. Therefore, the protocol can be executed if and only if both measurement results for the secret messages 10 and 11 are equal. By doing so, we find that $\alpha = \beta = \frac{1}{\sqrt{2}}$, which is turned out be the Bell states as given in Eq. (1).

Thus, initial states can be maximally or non-maximally entangled states depending upon the secret messages. Therefore, it is clear that Alice and Bob cannot send their secret messages irrespective of the initial states generated by Charlie. It is desirable to have a situation that secret messages of the communicants are independent of the initial states. Equivalently, we demand a situation that the initial states are chosen based on the secret messages. This is possible if and only if the communicants have the power to generate the maximally entangled initial states. By doing so, the role of the controller becomes insignificant, and we can have controller-independent bidirectional direct quantum communication. Having realized these points, the following protocol is being devised.

## 4 Controller-independent BQDC protocol

In this new protocol, Alice and Bob are capable of generating Bell states as their initial states. Here we describe how Alice and Bob can exchange their secret messages

**Table 2** Relation between Alice's (Bob's) measurement result $MR_A$ ($MR_B$), Charlie's initial states $IS$ and Bob's (Alice's) secret messages

| $MR_A$ | Bob's (Alice's) secret messages | | | |
|---|---|---|---|---|
| ($MR_B$) | 00 | 10 | 11 | 01 |
| $\|\omega^+\rangle = \alpha\|00\rangle + \beta\|11\rangle$ | $\|\omega^+\rangle$ | $\|\chi^+\rangle$ | $-\|\chi^-\rangle$ | $\|\omega^-\rangle$ |
| | ($\|\omega^+\rangle$) | ($\alpha\|10\rangle + \beta\|01\rangle$) | ($-\alpha\|10\rangle + \beta\|01\rangle$) | ($\|\omega^-\rangle$) |
| $\|\chi^+\rangle = \alpha\|01\rangle + \beta\|10\rangle$ | $\|\chi^+\rangle$ | $\|\omega^+\rangle$ | $\|\omega^-\rangle$ | $-\|\chi^-\rangle$ |
| | ($\|\chi^+\rangle$) | ($\alpha\|11\rangle + \beta\|00\rangle$) | ($-\alpha\|11\rangle + \beta\|00\rangle$) | ($\|\chi^-\rangle$) |
| $\|\chi^-\rangle = \alpha\|01\rangle - \beta\|10\rangle$ | $\|\chi^-\rangle$ | $\|\omega^-\rangle$ | $\|\omega^+\rangle$ | $-\|\chi^+\rangle$ |
| | ($\|\chi^-\rangle$) | ($\alpha\|11\rangle - \beta\|00\rangle$) | ($-\alpha\|11\rangle - \beta\|00\rangle$) | ($\|\chi^+\rangle$) |
| $\|\omega^-\rangle = \alpha\|00\rangle - \beta\|11\rangle$ | $\|\omega^-\rangle$ | $\|\chi^-\rangle$ | $-\|\chi^+\rangle$ | $\|\omega^+\rangle$ |
| | ($\|\omega^-\rangle$) | ($\alpha\|10\rangle - \beta\|01\rangle$) | ($-\alpha\|10\rangle - \beta\|01\rangle$) | ($\|\omega^+\rangle$) |

without depending on the controller, Charlie. The steps followed in the protocol are given in Fig. 2.

*Step 1* Alice prepares one of the Bell states as given in Eq. (1). The first particles of the Bell states belong to Alice and the second particles belong to Bob. It is known that two-bit secret messages {00, 01, 10, 11} are encoded as unitary operators $\{I, \sigma_z, \sigma_x, i\sigma_y\}$, respectively. Now Alice will perform the unitary operation according to her secret message on the Bell state chosen randomly and then she will announce the result to Bob.

Say, $A$ is the initial state [$A = |\phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$] prepared by Alice. If 01 is the secret message, she has to choose $\sigma_z$ as the unitary operator. After performing the unitary operation on $A$, she will be ensured with $A'$.

Therefore,

$$\sigma_z(|\phi^+\rangle) = \sigma_z\left\{\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)\right\} = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle) = |\phi^-\rangle = A'.$$

*Step 2* After receiving the operation result $A'$ from Alice, Bob will select one Bell state as an initial state according to his secret message and $A'$ by following Table 3. Say, 11 is the secret message and $|\phi^-\rangle$ is the operation result of Alice, then the initial state of Bob will be $|\psi^+\rangle$. Now Bob will announce the same result $A'$ to Alice. Note that no need for Bob to encode the initial state using the unitary operator.

*Step 3* If there is no eavesdropper, Alice will get the same result, i.e., $A'$ from Bob. Alice will perform a measurement on the received operation result from Bob with $A'$.

By doing so, if there is no eavesdropper she will be ensured with 1, else the measurement result will be 0. From this measurement result, Alice will check the presence of Eve. If there is an eavesdropper, i.e., if the measurement result is 0, then Alice will announce to abort the communication.

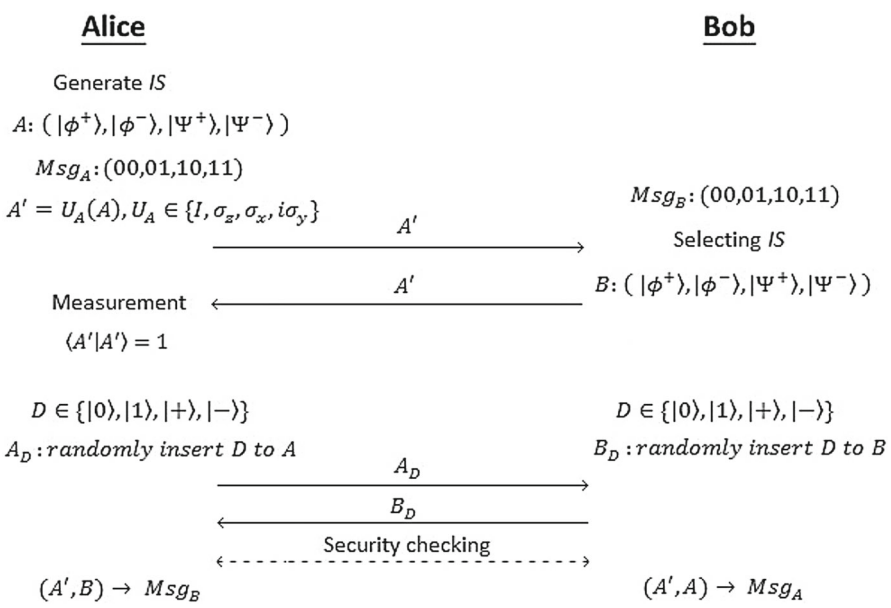


**Fig. 2** Controller-independent BQDC protocol

Alice measurement

$$\langle A'|A'\rangle = \delta \Rightarrow \langle|\phi^-\rangle||\phi^-\rangle\rangle = 1$$

If the measurement result is $\delta = 1$, then Alice and Bob will be confirmed with the absence of eavesdropper; otherwise, they will abort the communication.

*Step 4* For secure consideration, Alice and Bob will prepare a sufficient number of single particles $D$ in one of the four states$\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$, where $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ and $|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$. By inserting $D$ to the initial state $A$ and $B$, it will become $A_D$ and $B_D$, respectively. Alice and Bob then exchange the new states $A_D$ and $B_D$ to each other simultaneously and execute the security checking on $D$. If error rate goes beyond the threshold, they will abort the communication. Otherwise, they will proceed to the next step. Upon getting the initial state $B$ and $A$, Alice and Bob can deduce the secret messages of each other according to Table 3.

In the example of our discussion, we have

$$\begin{aligned}(A', B) \rightarrow Msg_B \Rightarrow \left(|\phi^-\rangle, |\psi^+\rangle\right) \rightarrow 11\\ (A', A) \rightarrow Msg_A \Rightarrow \left(|\phi^-\rangle, |\phi^+\rangle\right) \rightarrow 01\end{aligned}$$

Thus, the messages are secretly exchanged between Alice and Bob without the help of any controller.

**Table 3** Relation between Alice's secret messages, initial states and Bob's secret messages, initial states and their unitary operation results

| Alice's secret messages | Initial State (IS) | | | | Bob's secret messages |
|---|---|---|---|---|---|
| | $\|\phi^+\rangle$ | $\|\phi^-\rangle$ | $\|\psi^+\rangle$ | $\|\psi^-\rangle$ | |
| 00 | $\|\phi^+\rangle$ | $\|\phi^-\rangle$ | $\|\psi^+\rangle$ | $\|\psi^-\rangle$ | 00 |
| 01 | $\|\phi^-\rangle$ | $\|\phi^+\rangle$ | $\|\psi^-\rangle$ | $\|\psi^+\rangle$ | 01 |
| 10 | $\|\psi^+\rangle$ | $\|\psi^-\rangle$ | $\|\phi^+\rangle$ | $\|\phi^-\rangle$ | 10 |
| 11 | $\|\psi^-\rangle$ | $\|\psi^+\rangle$ | $\|\phi^-\rangle$ | $\|\phi^+\rangle$ | 11 |

## 5 Security analysis

This section shows that the proposed controller-independent BQDC is secure against two types of attacks: (i) intercept-and-resend attack and (ii) man-in-the-middle attack. Moreover, the proposed protocol will not tolerate any (iii) information leakage.

(i) *Intercept-and-resend attack* In the proposed protocol, Eve may attempt to play the role of Alice or Bob to read the secret message. In this case, the presence of an outsider can be realized by the measurement of Alice at the third step of the protocol. If Alice's measurement gives the wrong result, Alice will realize the presence of the third party and she will abort the communication. Thus, the intercept-and-resend attack is also avoided in this protocol.

(ii) *Man-in-the-middle attack* Suppose Eve prepares some Bell states with the intent to steal secret messages by using the non-local swap gate scheme [28]. When Charlie (controller) sends the sequence of $A$ particles and $B$ particles to Alice and Bob, Eve can intercept the $A$ sequence and $B$ sequence to effect the communication. As there is no controller in the proposed protocol, middle-man attack is not possible. Furthermore, if there is any middle-man attack during the exchange of states $A_D$ and $B_D$, the attack can be tracked by executing the security checking as mentioned in step 4.

(iii) *No information leakage* Suppose an outsider manages to know the initial Bell state of either Alice or Bob, the coding operation must be one of the four possibilities $\{I, \sigma_z, \sigma_x, i\sigma_y\}$ which contains $-4 \times \frac{1}{4}\log_2\frac{1}{4} = 2$ bits of secret information. Therefore, the proposed protocol does not permit information leakage either from Alice to Bob or from Bob to Alice. Hence, the protocol allows the full control of the users over their message.

Moreover, it is important to discuss the honesty of Alice and Bob. Most of the protocols have assumed that the legitimate users are honest and reliable and usually cooperate to decode the classical secret messages from each other. However, there is a problem involving the honesty of the users. If Alice suspects Bob as a malicious user, then she will not announce the initial state at all. As all the four initial states are possible for any given measurement results of Alice (refer Table 3), Bob cannot read the secret message of Alice. The entropy of permission will be $-4 \times \frac{1}{4}\log_2\frac{1}{4} = 2$ bits, and hence, Alice's secret message can be fully controlled by herself without the help of any controller. Besides that, in Chang et al. protocol neither Alice nor

Bob knows the initial state generated by Charlie. If Charlie is not a genuine arbiter, he can distribute the wrong sequence among Alice and Bob. As a result, they will exchange the wrong message and they will be aware of this only at the last step of the protocol. However, controller-independent protocol does not experience such types of disadvantages. Furthermore, there are attacks that use the imperfect quantum equipment to get illegal secret information, like the Trojan horse attack [29,30], which would be prevented when the technology of manufacturing quantum resource becomes more mature.

### 5.1 Qubit efficiency

Generally, qubit efficiency ($\eta$) of a quantum cryptographic protocol is defined as,

$$\eta = \frac{c}{q} \tag{3}$$

where $c$ is the total number of transmitted classical bits and $q$ is total number of qubits used in the protocol. However, there is a limitation to this measurement that it does not include the classical communication which is required for decoding the information in the controlled BQDC protocol. To avoid this limitation, Adan Cabello [24] proposed a new formula for qubit efficiency, which is defined as,

$$\eta = \frac{c}{q + b} \tag{4}$$

where $b$ denotes the number of classical bits exchanged for decoding of the secret message. Application of the above efficiency formula can be found in [26,27]. Note that no classical bits are being used for the extraction of the secret message and security checking process in Chang et al. protocol as well as in the proposed protocol.

In Chang et al. protocol, Charlie prepares $(n + l + d)$ Bell states for the transmission of two bits of classical information. So the number of qubits used for $n$ number of Bell state is $2m_1 = 2m_2$ (Say $2m_1 = 2m_2 = 2M$). $l$ and $d$ are the numbers for the first and second security checking for which $(2M + 2M)$ numbers of decoy qubits are used. Therefore, the total number of the qubit used in the protocol is $q = 2M + 4M = 6M$. We know that sender has to transmit a secret message (00, 01, 10, 11), which has two classical bits. If there are $M$ number of the secret message, then the total number of transmitted classical bit is $c = 2M$. However, in step 4, Alice and Bob are inserting $D$ to the initial state for security checking, which is single qubit. Thus, the final number of qubits used in this protocol is $q = 6M + 2$. Therefore, qubit efficiency of the protocol is

$$\eta = \frac{c}{q} = \frac{2M}{6M + 2} \cong \frac{2M}{6M} \cong 33.33\%$$

In the proposed protocol, Alice prepares $n$ number of Bell states and Bob is having $n$ number of Bell states for the selection of initial state. Therefore, $q = 4M$. As the

secret message is same for all protocol, $c = 2M$. Alice and Bob are inserting $D$ to the initial state for security checking in this case also. Therefore, $q = 4M + 2$.

$$\eta = \frac{c}{q} = \frac{2M}{4M+2} \cong \frac{2M}{4M} \cong 50\%$$

Thus, quantum efficiency of controller-independent BDQC protocol is more than that of controlled BDQC protocol, namely Chang et al. protocol.

## 6 Conclusion

The first result of this work exhibits the importance of Bell states, which are being used as initial states in Chang et al. protocol. It is to be emphasized that maximally entangled states can *only* be used as initial states so that the communicants can choose their secret messages irrespective of the initial states generated by the controller. On the other hand, initial states can be chosen based on the secret messages, if the communicants are empowered with generating maximally entangled Bell states. In this case, the controller becomes insignificant.

In proposed protocol, Alice and Bob are proficient of generating initial states according to their secret messages. This protocol does not require single particle encoding due to the adopted procedure. Security analysis reveals that the intercept-and-resend attack and man-in-the-middle attack are not possible at any step of the protocol and information leakage between the communicants is also not possible in this proposal. Thus, the proposed controller-independent bidirectional quantum communication protocol is like a *conversion* between two persons without the help of any third person. Both the communicants have full control over their secret messages. If any one of the communicants suspects the other, he or she can abort the communication without disclosing the initial Bell state. Further, the third party cannot read the message without knowing the initial state and the presence of the third party can be detected by the communicants. Further, quantum efficiency of the protocol is higher compared to the Cheng et al. protocol. Moreover, the proposed protocol can be extended to a multiparty case as the sender has the power to communicate with any communicant without the help of a controller. In short, the controller-independent bidirectional quantum direct communication protocol is a new scheme of quantum communication with higher level of security and efficiency when compared to the existing controlled bidirectional quantum direct communication protocols.

## References

1. Bennett, C.H., Brassard, G.: Quantum cryptography: public key distribution and coin tossing. In: Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, pp. 175–179 (1984)
2. Bostrom, K., Felbinger, T.: Deterministic secure direct communication using entanglement. Phys. Rev. Lett. **89**, 187902 (2002)
3. Deng, F.G., Long, G.L., X S, Liu: Two-step quantum direct communication protocol using the Einstein–Podolsky–Rosen pair block. Phys. Rev. A **68**, 042317 (2003)

4. Deng, F.G., Long, G.L.: Secure direct communication with a quantum one-time pad. Phys. Rev. A **69**, 052319 (2004)
5. Zhang, Z.J.: Multiparty quantum secret sharing of secure direct communication. Phys. Lett. A **342**, 60–66 (2005)
6. Nguyen, B.A.: Quantum dialogue. Phys. Lett. A **328**(1), 6–10 (2004)
7. Man, Z.X., Zhang, Z.J., Li, Y.: Quantum dialogue revisited. Chin. Phys. Lett. **22**(1), 22–24 (2005)
8. Xia, Y., Fu, C.B., Zhang, S., Hong, S.K., Yeon, K.H., Um, C.L.: Quantum dialogue by using GHZ state. J. Korean Phys. Soc. **48**(1), 24–27 (2006)
9. Man, Z.X., Xia, Y.J., Zhang, Z.J.: Secure deterministic bidirectional communication without entanglement. Int. J. Quantum Inf. **4**(4), 739–746 (2006)
10. Yang, Y.G., Wen, Q.Y.: Quasi-secure quantum dialogue using single photons. Sci. Chin. Ser. G Phys. Mech. Astron. **50**(5), 558–562 (2007)
11. Ji, X., Zhang, S.: Secure quantum dialogue based on single-photon. Chin. Phys. **15**(7), 1418–1420 (2006)
12. Chen, Y., Man, Z.X., Xia, Y.J.: Quantum bidirectional secure direct communication via entanglement swapping. Chin. Phys. Lett. **24**(1), 19–22 (2007)
13. Tan, Y.G., Cai, Q.Y.: Classical correlation in quantum dialogue. Int. J. Quantum Inf. **6**(2), 325–329 (2008)
14. Gao, F., Guo, F.Z., Wen, Q.Y., Zhu, F.C.: Revisiting the security of quantum dialogue and bidirectional quantum secure direct communication. Sci. Chin. Ser. G Phys. Mech. Astron. **51**(5), 559–566 (2008)
15. Dong, L., Xiu, X.M., Gao, Y.J., Chi, F.: Quantum dialogue protocol using a class of three-photon W states. Commun. Theor. Phys. **52**(5), 853–856 (2009)
16. Luo, Y.-P., Lin, C.-Y., Hwang, T.: Efficient quantum dialogue using single photons. Quantum Inf. Process. **13**(11), 2451–2461 (2014)
17. Man, Z.X., Xia, Y.J.: Controlled bidirectional quantum direct communication by using a GHZ state. Chin. Phys. Lett. **23**(7), 1680–1682 (2006)
18. Xia, Y., Song, J., Nie, J., Song, H.S.: Controlled secure quantum dialogue using a pure entangled GHZ states. Commun. Theor. Phys. **48**(5), 841–846 (2007)
19. Chen, X.B., Wen, Q.Y., Guo, F.Z., Sun, Y., Xu, G., Zhu, F.C.: Controlled quantum secure direct communication with W-state. Int. J. Quantum Inf. **6**, 899 (2008)
20. Ye, T.Y., Jiang, L.Z.: Improvement of controlled bidirectional quantum direct communication using a GHZ state. Chin. Phys. Lett. **30**(4), 040305 (2013)
21. Liu, Z.-H., Chen, H.-W.: Comment on "Improvement of controlled bidirectional quantum direct communication using a GHZ state". Chin. Phys. Lett. **30**(7), 079901 (2013)
22. Ye, T.-Y., Jiang, L.-Z.: Reply to the comment on "Improvement of controlled bidirectional quantum direct communication using a GHZ state". Chin. Phys. Lett. **30**(7), 079902 (2013)
23. Chang, C.-H., Luo, Y.-P., Yang, C.-W., Hwang, T.: Intercept-and-resend attack on controlled bidirectional quantum direct communication and its improvement. Quantum Inf. Process. **14**, 3515–3522 (2015)
24. Cabello, A.: Quantum key distribution in the Holevo limit. Phys. Rev. Lett. **85**, 5635–5638 (2000)
25. Hassanpour, S., Houshmand, M.: Efficient controlled quantum secure direct communication based on GHZ-like states. Quantum Inf. Process. **14**, 739 (2015)
26. Pathak, A.: Efficient protocols for unidirectional and bidirectional controlled deterministic secure quantum communication: different alternative approaches. Quantum Inf. Process. **14**, 2195–2210 (2015)
27. Yu, Z.B., Gong, L.H., Wen, R.H.: Novel multiparty controlled bidirectional quantum secure direct communication based on continuous-variable states. Int. J. Theor. Phys. **55**, 1447–1459 (2016)
28. Chou, Y.-H., Lin, Y.-T., Zeng, G.-J., Lin, F.-J., Chen, C.-Y.: Controlled bidirectional quantum secure direct communication. Sci. World J. **2014**, 694798 (2014). doi:10.1155/2014/694798
29. Gisin, N., Ribordy, G., Tittel, W., Zbinden, H.: Quantum cryptography. Rev. Mod. Phys. **74**(1), 145–195 (2002)
30. Gisin, N., Fasel, S., Kraus, B., Zbinden, H., Ribordy, G.: Trojan-horse attacks on quantum-key-distribution systems. Phys. Rev. A At. Mol. Opt. Phys. **73**(2), 022320 (2006)