Controlled mutual quantum entity authentication using entanglement swapping*

Min-Sung Kang[a)b)], Chang-Ho Hong[a)b)], Jino Heo[a)b)], Jong-In Lim[a)b)], and Hyung-Jin Yang[a)b)c)†]

[a)] *Center for Information Security Technologies (CIST), Korea University, Seoul, South Korea*
[b)] *Graduate School of Information Security, Korea University, Anam 5-ga Sungbuk-gu, Seoul, South Korea*
[c)] *Department of Physics, Korea University, Sejong, 339-700, South Korea*

(Received 31 January 2015; revised manuscript received 3 February 2015; published online 3 August 2015)

In this paper, we suggest a controlled mutual quantum entity authentication protocol by which two users mutually certify each other on a quantum network using a sequence of Greenberger–Horne–Zeilinger (GHZ)-like states. Unlike existing unidirectional quantum entity authentication, our protocol enables mutual quantum entity authentication utilizing entanglement swapping; moreover, it allows the managing trusted center (TC) or trusted third party (TTP) to effectively control the certification of two users using the nature of the GHZ-like state. We will also analyze the security of the protocol and quantum channel.

Keywords: quantum authentication, quantum cryptography, quantum communication, GHZ-like state

PACS: 03.67.Dd, 03.67.Hk, 03.67.Ac, 03.65.Ud **DOI:** 10.1088/1674-1056/24/9/090306

1. Introduction

In network communication, it is very important to develop a system or protocol in which transferred information is received by only the authenticated user. The receiver identifies the creator of the information and verifies whether it was falsified. Authentication provides secure network communication by certifying messages, entities, and keys. In particular, entity authentication, such as password authentication, one-time password authentication, challenge-response authentication, bit commitment, and so on, refers to a series of processes for certifying entity identification.[1–4]

When identification[1] is used as entity authentication it refers to verification, identity confirmation, or identity certification in a narrow sense, such as a user identification code, user name, user ID, or ID number, which are used to verify the authenticated user in a multiuser computer environment or communication network system. In a broad sense, it is a form of identification certification that is required for accessing online information service systems, such as online databases. To access and log into the network, the user ID and corresponding password or key are always necessary to accurately verify the identification. For example, at the International Organization for Standardization (ISO) and the International Electro-technical Commission (IEC), only entity authentication, specifically the meaning of a series of phrases, is used to verify identity.[5]

Since Bennett and Brassard suggested quantum key distribution,[6] many researchers of quantum communication protocols have suggested quantum entity authentication protocols[7–11] under the names of quantum identification or quantum identity authentication, as well as multiparty simultaneous quantum entity protocols,[12–16] in which a trusted center (TC) or trusted third party (TTP) effectively certify users in the quantum network. Furthermore, various bidirectional quantum communication protocols[17–28] for bilaterally transmitting or sharing quantum information, such as bidirectional quantum key distribution, bidirectional quantum communication, bidirectional quantum teleportation, and bidirectional quantum secret sharing, have been proposed.

Based on the above bidirectional quantum communication protocols, we conceived a bidirectional quantum entity authentication protocol using entanglement swapping. In this protocol, TC (or TTP) can control all of the mutual authentication phases, including entanglement swapping in a quantum network[29–34] which utilizes Greenberger–Horne–Zeilinger (GHZ)-like states, as in controlled quantum teleportation protocols,[35–37] quantum secret sharing protocols,[38–41] controlled direct communication,[42,43] and remote state preparation.[44] To enhance security, TC (or TTP) randomly inserts a decoy qubit before the entity authentication of two users.[45,46]

2. Entity authentication

In the entity authentication protocol, an entity is commonly referred to as an individual or a machine, an entity that attempts to prove its identity is a prover or claimant, and an entity that verifies another's identity is a verifier. One of several authentication protocols, challenge-response authentication is

*Project supported by the Research Foundation of Korea University.
†Corresponding author. E-mail: yangh@korea.ac.kr
© 2015 Chinese Physical Society and IOP Publishing Ltd

widely used in classical entity authentication.

Challenge-response authentication can be designed using a symmetric-key cipher, asymmetric-key cipher, digital signature, and keyed-hash functions.[1–4] Figure 1 depicts a simple example of challenge-response authentication using a symmetric-key cipher.

The nonce (random number), R_B, and timestamp T in Figs. 1(a) and 1(b) are used to maintain the freshness of the entity authentication process, which differs from message authentication. Message authentication is completed by verifying the message integrity and identifying the message generator. In entity authentication, on the other hand, the entity attempting access of the network system is to be authenticated in real time; accordingly, freshness or timeliness is indispensable. In contrast, most quantum communication is achieved in a short time period; it is therefore not necessary to consider freshness or timeliness in quantum entity authentication. This marks the difference between classical entity authentication and quantum entity authentication.

By adding authentication processes to the unidirectional authentication shown in Fig. 1, bidirectional authentication is additionally possible, as shown in Fig. 2.[1–4]

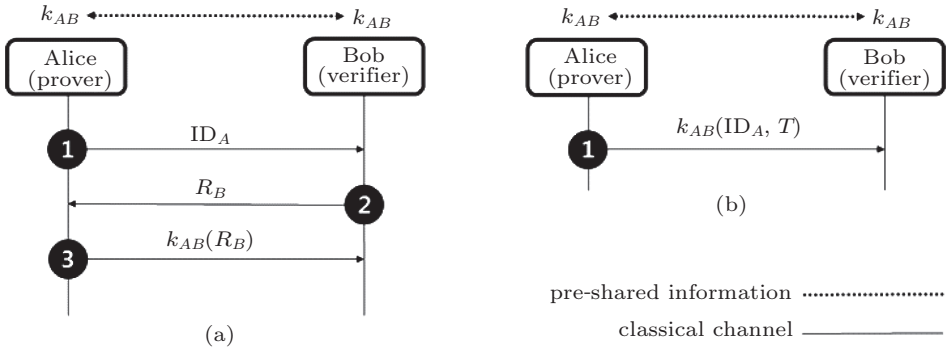


Fig. 1. Challenge-response authentication using a symmetric-key cipher.[1–4] In phase 1 in panel (a), prover Alice transmits her identification ID_A to verifier Bob to request entity authentication. In challenge phase 2 of panel (a) Bob sends a nonce (random number) R_B to Alice. In response phase 3 of panel (a), Alice demonstrates that she is sharing the secret key, k_{AB}, with Bob by transmitting to Bob the encrypted random number, $k_{AB}(R_B)$. The nonce, R_B, is renewed in each session. In panel (b), Alice shows that she is also sharing the secret key, k_{AB}, with Bob. Unlike Bob, Alice completes the entity authentication by transmitting only once the encrypted number, $k_{AB}(\mathrm{ID}_A, T)$, of her identification ID_A and timestamp T using the secret key, k_{AB}. If timestamp T is not agreed upon in advance, Bob rejects Alice's authentication.

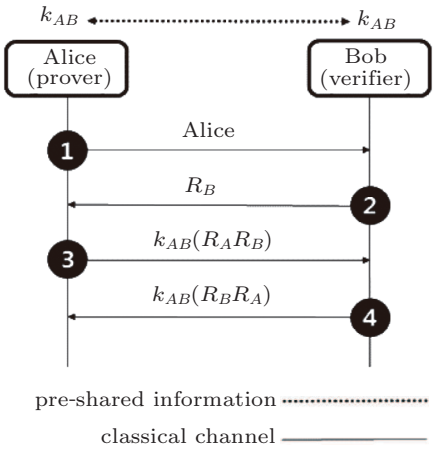


Fig. 2. Bidirectional challenge-response authentication using a symmetric-key cipher.[1–4] As in Fig. 1(a), Alice and Bob, respectively, check the nonce (random number) R_A and R_B, and mutually verify the unidirectional authentication using the nonce. In phase 3, Alice generates encrypted random numbers $k_{AB}(R_AR_B)$ and responds to Bob's challenge, while simultaneously challenging Bob to identification. In phase 4, Bob generates $k_{AB}(R_BR_A)$ and responds to Alice's challenge, thereby completing the certification process.

3. Entangled states and entanglement swapping

3.1. Bell states and entanglement swapping

Four mutually orthonormal Bell states are expressed as follows:

$$|\Phi^{\pm}\rangle = \frac{1}{\sqrt{2}}(|00\rangle \pm |11\rangle), \quad |\Psi^{\pm}\rangle = \frac{1}{\sqrt{2}}(|01\rangle \pm |10\rangle), \quad (1)$$

where $|0\rangle$ and $|1\rangle$ are two eigenstates of Pauli operator σ_z or horizontally and vertically polarized states of the photon, respectively.

Quantum entanglement swapping plays an important role in quantum communication. Using quantum entanglement swapping, we can establish two entangled quantum systems without direct interaction. Suppose that Alice prepares $|\Psi^+\rangle_{1A1B}$ and $|\Psi^+\rangle_{2A2B}$, and sends Bob two qubits, $1B$ and $2B$. Then, two distant users, Alice and Bob, share two entangled states, $|\Psi^+\rangle_{1A1B} \otimes |\Psi^+\rangle_{2A2B}$, where Alice has qubits $1A$ and $2A$, and Bob has $1B$ and $2B$. This state can be rearranged as follows:

$$\begin{aligned} &|\Psi^+\rangle_{1A1B} \otimes |\Psi^+\rangle_{2A2B} \\ &= \frac{1}{2}(|\Phi^+\rangle_{1A2A}|\Phi^+\rangle_{1B2B} - |\Phi^-\rangle_{1A2A}|\Phi^-\rangle_{1B2B} \\ &\quad + |\Psi^+\rangle_{1A2A}|\Psi^+\rangle_{1B2B} - |\Psi^-\rangle_{1A2A}|\Psi^-\rangle_{1B2B}). \end{aligned} \quad (2)$$

If Alice measures qubits $1A$ and $2A$ with the Bell basis, $|\Psi^+\rangle_{1A1B} \otimes |\Psi^+\rangle_{2A2B}$ in Eq. (2) collapses into $|\Phi^+\rangle_{1A2A}|\Phi^+\rangle_{1B2B}$, $|\Phi^-\rangle_{1A2A}|\Phi^-\rangle_{1B2B}$, $|\Psi^+\rangle_{1A2A}|\Psi^+\rangle_{1B2B}$, or $|\Psi^-\rangle_{1A2A}|\Psi^-\rangle_{1B2B}$ by equal probability of 1/4. Due to the Bell measurement, the entanglements

between qubits $1A$ and $1B$, and between qubits $2A$ and $2B$, are swapped to entanglements between qubits $1A$ and $2A$, and between qubits $1B$ and $2B$.[12,21,31] Figure 3 illustrates the entanglement swapping of Bell states in three steps. The Bell measurement outcomes on four different initial combinations of Bell states are summarized in Table 1.

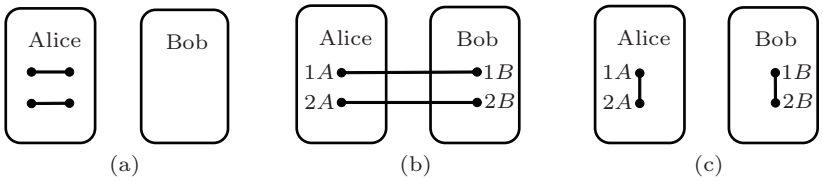


Fig. 3. Schematic representation of the entanglement swapping of Bell states. (a) Alice prepares two entangled states. A dot (•) represents each qubit and a line (−) denotes entanglements. (b) Alice sends Bob one qubit in each entanglement pair. (c) Alice and Bob respectively perform Bell measurements on each of their own qubits. Consequently, the entanglements between Alice and Bob are swapped.[23]

Table 1. Measurement outcomes of the entanglement swapping on sixteen combinations of four Bell states.

	$\|\Phi^+\rangle_{2A2B}$	$\|\Phi^-\rangle_{2A2B}$	$\|\Psi^+\rangle_{2A2B}$	$\|\Psi^-\rangle_{2A2B}$
$\|\Phi^+\rangle_{1A1B}$	ID + +	ID + −	Rev + +	Rev + −
$\|\Phi^-\rangle_{1A1B}$	ID + −	ID + +	Rev + −	Rev + +
$\|\Psi^+\rangle_{1A1B}$	Rev + +	Rev + −	ID + +	ID + −
$\|\Psi^-\rangle_{1A1B}$	Rev + −	Rev + +	ID + −	ID + +

The symbol ID + + denotes the set of four possible outcomes $\{(|\Phi^+\rangle_{1A2A}, |\Phi^+\rangle_{1B2B}), (|\Phi^-\rangle_{1A2A}, |\Phi^-\rangle_{1B2B}), (|\Psi^+\rangle_{1A2A}, |\Psi^+\rangle_{1B2B})$, and $(|\Psi^-\rangle_{1A2A}, |\Psi^-\rangle_{1B2B})\}$ with an equal probability of 1/4. Similarly, ID + − represents $\{(|\Psi^+\rangle_{1A2A}, |\Psi^-\rangle_{1B2B})$ $(|\Phi^-\rangle_{1A2A}, |\Phi^+\rangle_{1B2B}), (|\Phi^+\rangle_{1A2A}, |\Phi^-\rangle_{1B2B})$, and $(|\Psi^-\rangle_{1A2A}, |\Psi^+\rangle_{1B2B})\}$, and Rev + + symbolizes $\{(|\Phi^+\rangle_{1A2A}, |\Psi^+\rangle_{1B2B}), (|\Phi^-\rangle_{1A2A}, |\Psi^-\rangle_{1B2B}), (|\Psi^+\rangle_{1A2A}, |\Phi^+\rangle_{1B2B})$, and $(|\Psi^-\rangle_{1A2A}, |\Phi^-\rangle_{1B2B})\}$. Rev + − describes $\{(|\Phi^+\rangle_{1A2A}, |\Psi^-\rangle_{1B2B})$ $(|\Phi^-\rangle_{1A2A}, |\Psi^+\rangle_{1B2B}), (|\Psi^+\rangle_{1A2A}, |\Phi^-\rangle_{1B2B})$, and $(|\Psi^-\rangle_{1A2A}, |\Phi^+\rangle_{1B2B})\}$.[23,47]

3.2. GHZ-like state and entanglement swapping

A GHZ-like state consisting of

$$|x+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \quad \text{and} \quad |x-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

is expressed as follows:[26,32]

$$\begin{aligned}|\xi\rangle_{123} &= \frac{1}{\sqrt{2}}(|x+\rangle|x+\rangle|x+\rangle + |x-\rangle|x-\rangle|x-\rangle)_{123}\\ &= \frac{1}{4}[(|0\rangle + |1\rangle)\otimes(|0\rangle + |1\rangle)\otimes(|0\rangle + |1\rangle)\\ &\quad -(|0\rangle - |1\rangle)\otimes(|0\rangle - |1\rangle)\otimes(|0\rangle - |1\rangle)]_{123}\\ &= \frac{1}{2}(|001\rangle + |010\rangle + |100\rangle + |111\rangle)_{123}, \end{aligned} \tag{3}$$

where $|x+\rangle$ and $|x-\rangle$ are two eigenstates of σ_x, and $|0\rangle$ and $|1\rangle$ are eigenstates of σ_z. Another GHZ-like state consisting of

$$|y+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + \mathrm{i}|1\rangle) \quad \text{and} \quad |y-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - \mathrm{i}|1\rangle)$$

is represented as follows:

$$\begin{aligned}|\varepsilon\rangle_{123} &= \frac{1}{\sqrt{2}}(|y+\rangle|y+\rangle|y+\rangle + |y-\rangle|y-\rangle|y-\rangle)_{123}\\ &= \frac{1}{4}[(|0\rangle + \mathrm{i}|1\rangle)\otimes(|0\rangle + \mathrm{i}|1\rangle)\otimes(|0\rangle + \mathrm{i}|1\rangle)\\ &\quad +(|0\rangle - \mathrm{i}|1\rangle)\otimes(|0\rangle - \mathrm{i}|1\rangle)\otimes(|0\rangle - \mathrm{i}|1\rangle)]_{123}\\ &= \frac{1}{2}(|000\rangle - |011\rangle - |101\rangle - |110\rangle)_{123}, \end{aligned} \tag{4}$$

where $|y+\rangle$ and $|y-\rangle$ are two eigenstates of σ_y. Various GHZ-like states can be generated, as shown in Table 2.

Table 2. Various GHZ-like states: $|x+\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$ and $|x-\rangle = (|0\rangle - |1\rangle)/\sqrt{2}$ are eigenstates of Pauli operator σ_x, $|y+\rangle = (|0\rangle + \mathrm{i}|1\rangle)/\sqrt{2}$ and $|y-\rangle = (|0\rangle - \mathrm{i}|1\rangle)/\sqrt{2}$ are eigenstates of Pauli operator σ_y.

$(\|x+\rangle\|x+\rangle\|x\pm\rangle + \|x-\rangle\|x-\rangle\|x\mp\rangle)/\sqrt{2} = (\|\Phi^+\rangle_{12}\|0\rangle_3 \pm \|\Psi^+\rangle_{12}\|1\rangle_3)/\sqrt{2}$
$(\|x\pm\rangle\|x\mp\rangle\|x+\rangle + \|x\mp\rangle\|x\pm\rangle\|x-\rangle)/\sqrt{2} = (\|\Phi^-\rangle_{12}\|0\rangle_3 \mp \|\Psi^-\rangle_{12}\|1\rangle_3)/\sqrt{2}$
$(\|x+\rangle\|x+\rangle\|x\pm\rangle - \|x-\rangle\|x-\rangle\|x\mp\rangle)/\sqrt{2} = (\|\Psi^+\rangle_{12}\|0\rangle_3 \pm \|\Phi^+\rangle_{12}\|1\rangle_3)/\sqrt{2}$
$(\|x\pm\rangle\|x\mp\rangle\|x+\rangle - \|x\mp\rangle\|x\pm\rangle\|x-\rangle)/\sqrt{2} = \mp(\|\Psi^-\rangle_{12}\|0\rangle_3 \mp \|\Phi^-\rangle_{12}\|1\rangle_3)/\sqrt{2}$
$(\|y+\rangle\|y+\rangle\|y\pm\rangle + \|y-\rangle\|y-\rangle\|y\mp\rangle)/\sqrt{2} = (\|\Phi^-\rangle_{12}\|0\rangle_3 \mp \|\Psi^+\rangle_{12}\|1\rangle_3)/\sqrt{2}$
$(\|y\pm\rangle\|y\mp\rangle\|y+\rangle + \|y\mp\rangle\|y\pm\rangle\|y-\rangle)/\sqrt{2} = (\|\Phi^+\rangle_{12}\|0\rangle_3 \pm \|\Psi^-\rangle_{12}\|1\rangle_3)/\sqrt{2}$
$(\|y+\rangle\|y+\rangle\|y\pm\rangle - \|y-\rangle\|y-\rangle\|y\mp\rangle)/\sqrt{2} = \mathrm{i}(\|\Psi^+\rangle_{12}\|0\rangle_3 \pm \|\Phi^-\rangle_{12}\|1\rangle_3)/\sqrt{2}$
$(\|y\pm\rangle\|y\mp\rangle\|y+\rangle - \|y\mp\rangle\|y\pm\rangle\|y-\rangle)/\sqrt{2} = \mp\mathrm{i}(\|\Psi^-\rangle_{12}\|0\rangle_3 \mp \|\Phi^+\rangle_{12}\|1\rangle_3)/\sqrt{2}$

By utilizing GHZ-like states in quantum information transmission or quantum communication, we can add a controller that controls or regulates the communication between two users. In practice, GHZ-like states have been used in controlled quantum teleportation protocols,[35–37] quantum secret sharing protocols,[38–41] controlled direct communication,[42,43] and remote state preparation.[44] We can understand how TC (or TTP) is authorized as a controller in controlled quantum teleportation or controlled secure direct communication by rearranging the GHZ-like state in three different forms as follows:

$$|\xi\rangle_{123} = \begin{cases} \dfrac{1}{\sqrt{2}}(|0\rangle_1|\Psi^+\rangle_{23} + |1\rangle_1|\Phi^+\rangle_{23}), \\ \dfrac{1}{\sqrt{2}}(|0\rangle_2|\Psi^+\rangle_{13} + |1\rangle_2|\Phi^+\rangle_{13}), \\ \dfrac{1}{\sqrt{2}}(|\Psi^+\rangle_{12}|0\rangle_3 + |\Phi^+\rangle_{12}|1\rangle_3). \end{cases} \tag{5}$$

If TC measures the first qubit in Eq. (5) in a σ_z basis, then the second and third-qubits will have a 50% chance of being in

an entangled state, $|\Psi^+\rangle_{23}$ or $|\Phi^+\rangle_{23}$. Therefore, the entangled state of two users who share the second and third qubits is determined by the measurement result of the controller who owns the first qubit.

Let us consider a composite system consisting of two GHZ-like states and an entanglement swapping on it. After performing a von Neumann measurement on one qubit of each GHZ-like state, we execute the entanglement swapping operation on the two Bell states as follows.

(I) A composite system of two GHZ-like states $|\xi\rangle_{123}$ and $|\xi\rangle_{456}$ are constructed as follows:

$$\begin{aligned}|\xi\rangle_{123}\otimes|\xi\rangle_{456} &= \frac{1}{2}(|001\rangle+|010\rangle+|100\rangle+|111\rangle)_{123}\\ &\otimes\frac{1}{2}(|001\rangle+|010\rangle+|100\rangle+|111\rangle)_{456}\\ &= \frac{1}{\sqrt{2}}(|\Psi^+\rangle_{12}|0\rangle_3+|\Phi^+\rangle_{12}|1\rangle_3)\\ &\otimes\frac{1}{\sqrt{2}}(|\Psi^+\rangle_{45}|0\rangle_6+|\Phi^+\rangle_{45}|1\rangle_6). \qquad (6)\end{aligned}$$

(II) If the third and sixth qubits of state $|\xi\rangle_{123}\otimes|\xi\rangle_{456}$ are measured in a σ_z basis, it will be collapsed to one of $|\Psi^+\rangle_{12}|\Psi^+\rangle_{45}$, $|\Psi^+\rangle_{12}|\Phi^+\rangle_{45}$, $|\Phi^+\rangle_{12}|\Psi^+\rangle_{45}$, or $|\Phi^+\rangle_{12}|\Phi^+\rangle_{45}$ by a 25% probability, as shown in Table 3.

(III) We perform the entanglement swapping operation on the two entangled states in Table 3 as previously mentioned; the result is the same as that in Table 2.

Table 3. If the third and sixth qubits of the composite system $|\xi\rangle_{123}\otimes|\xi\rangle_{456}$ are measured in a σ_z basis, then $|\xi\rangle_{123}\otimes|\xi\rangle_{456}$ will be collapsed into $|\Psi^+\rangle_{12}|\Psi^+\rangle_{45}$, $|\Psi^+\rangle_{12}|\Phi^+\rangle_{45}$, $|\Phi^+\rangle_{12}|\Psi^+\rangle_{45}$, or $|\Phi^+\rangle_{12}|\Phi^+\rangle_{45}$ by a 25% probability.

Measurement outcome	$\|0\rangle_6$	$\|1\rangle_6$
$\|0\rangle_3$	$\|\Psi^+\rangle_{12}\|\Psi^+\rangle_{45}$	$\|\Psi^+\rangle_{12}\|\Phi^+\rangle_{45}$
$\|1\rangle_3$	$\|\Phi^+\rangle_{12}\|\Psi^+\rangle_{45}$	$\|\Phi^+\rangle_{12}\|\Phi^+\rangle_{45}$

In addition to the above operation on the state in Eq. (5), various entanglement swapping operations on the 16 GHZ-like states in Table 2 are also possible.

4. Controlled mutual quantum entity authentication

Suppose that two users, Alice and Bob, want to certify each other in the quantum network; the TC (TTP), Charlie, controls or regulates the mutual entity authentication between them. The controlled mutual quantum entity authentication consists of the respective prepare, security check and the entity authentication phases. Figure 4 schematically illustrates the protocol of the controlled mutual quantum entity authentication that we suggest.

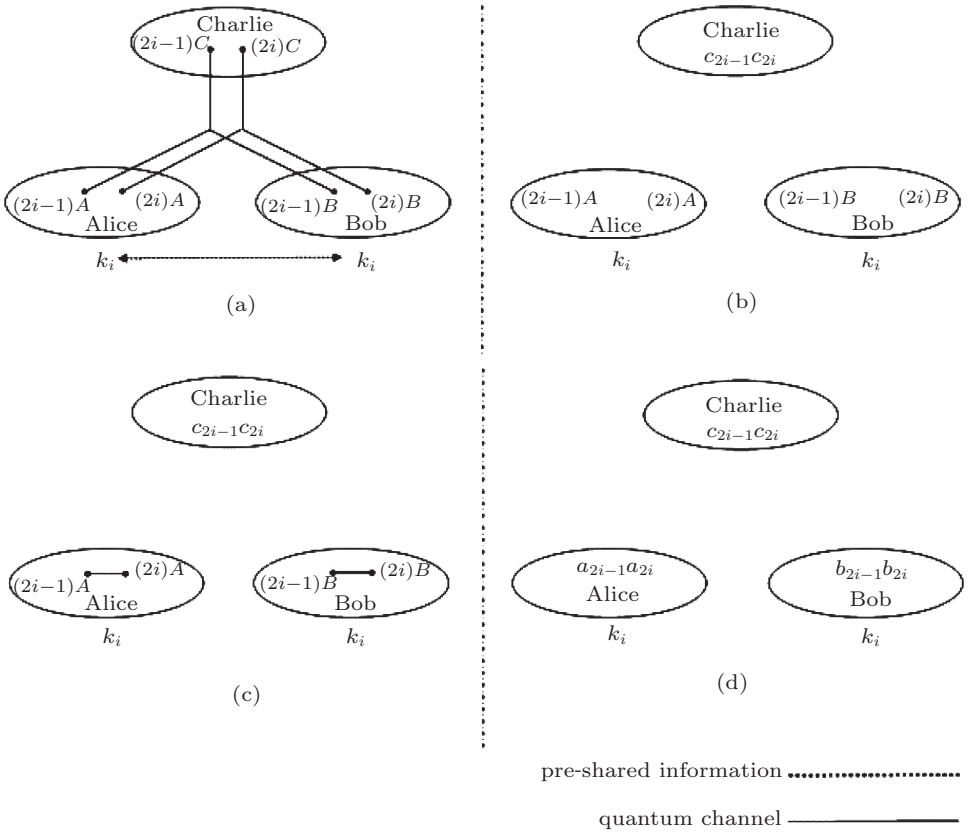


Fig. 4. (color online) Schematic representation of controlled mutual quantum entity authentication. (a) Alice and Bob share secret information k_i for entity authentication. Alice, Bob, and Charlie share the GHZ-like states $\otimes_{i=1}^{N}|\xi\rangle_{iAiBiC}$, which Charlie prepared in advance. (b) Charlie gains the classical bit, $c_{2i-1}c_{2i}$, which corresponds to the measurement outcome by the von Neumann measurement. Alice and Bob share one pair of Bell states with Charlie's measurement. (c) and (d) Alice and Bob swap one pair of the shared entangled states and, respectively, gain classical bit $a_{2i-1}a_{2i}$ and $b_{2i-1}b_{2i}$ as measurement outcomes. Subsequently, as shown in phase E4, Alice and Bob carry out mutual entity authentication under Charlie's control.

4.1. Preparation phase

P1 Alice and Bob share a secret key sequence, $K_{AB} = (k_1, k_2, \ldots, k_N)$, using QKD protocols,[6,48] which securely distribute the keys.[49,50] The sequence, $K_{AB} = (k_1, k_2, \ldots, k_N)$, is a classical bit sequence with the size of $2N$; the elements are defined as $k_i \in \{00, 01, 10, 11\}$. Key k_i corresponds to Pauli operators, as follows:

$$\begin{aligned} &k_i = 00 : U_{00} = I = |0\rangle\langle 0| + |0\rangle\langle 0|, \\ &k_i = 01 : U_{01} = \sigma_x = |1\rangle\langle 0| + |0\rangle\langle 1|, \\ &k_i = 10 : U_{10} = \mathrm{i}\sigma_y = |0\rangle\langle 1| - |1\rangle\langle 0|, \\ &k_i = 11 : U_{11} = \sigma_z = |0\rangle\langle 0| - |1\rangle\langle 1|. \end{aligned} \tag{7}$$

In our protocol, k_i is the secret information for the mutual entity authentication of Alice and Bob.

P2 The controller, Charlie, prepares the sequence $(|\xi\rangle_1, |\xi\rangle_2, \ldots, |\xi\rangle_{N_E})$ consisting of N GHZ-like states follows Refs. [51]–[58] for entity authentication, which is shown as

$$\begin{aligned} |\xi\rangle_{(2i-1)123} &= \frac{1}{\sqrt{2}}(|x+\rangle|x+\rangle|x+\rangle - |x-\rangle|x-\rangle|x-\rangle)_{(2i-1)123} \\ &= \frac{1}{\sqrt{2}}(|\Psi^+\rangle_{(2i-1)12}|0\rangle_{(2i-1)3} \\ &\quad + |\Phi^+\rangle_{(2i-1)12}|1\rangle_{(2i-1)3}), \end{aligned} \tag{8}$$

$$\begin{aligned} |\varepsilon\rangle_{(2i)123} &= \frac{1}{\sqrt{2}}(|y+\rangle|y+\rangle|y+\rangle + |y-\rangle|y-\rangle|y-\rangle)_{(2i)123} \\ &= \frac{1}{\sqrt{2}}(|\Phi^-\rangle_{(2i)12}|0\rangle_{(2i)3} - |\Psi^+\rangle_{(2i)12}|1\rangle_{(2i)3}). \end{aligned} \tag{9}$$

Charlie retains the third qubit, sends Alice the first qubit and Bob the second qubit, and then announces that he has transmitted the qubits to them. After transmission, the state is given as follows:

$$\begin{aligned} &|\xi\rangle_{(2i-1)ABC} \otimes |\varepsilon\rangle_{(2i)ABC} \\ &= \frac{1}{\sqrt{2}}(|\Psi^+\rangle_{(2i-1)AB}|0\rangle_{(2i-1)C} + |\Phi^+\rangle_{(2i-1)AB}|1\rangle_{(2i-1)C}) \\ &\quad \otimes \frac{1}{\sqrt{2}}(|\Phi^-\rangle_{(2i)AB}|0\rangle_{(2i)C} - |\Psi^+\rangle_{(2i)AB}|1\rangle_{(2i)C}). \end{aligned} \tag{10}$$

The subscript i in Eq. (10) designates the order in the sequence of the GHZ-like state, A, B, or C, showing the owner of the qubit. Transmitting N GHZ-like states to Alice and Bob, Charlie randomly inserts N_C decoy qubits

$$|x+\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}} \quad \text{or} \quad |x-\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}}$$

to detect the eavesdropping.[45,46] Alice and Bob, who received the qubits from Charlie, notify each communication member through the public channel of their safe receipt.

4.2. Security checking phase

S1 Confirming that Alice and Bob have safely received the qubit sequence, Charlie reveals the location of the decoy qubits.

S2 Alice and Bob execute the σ_x basis $\{|x+\rangle, |x-\rangle\}$ measurement only on the decoy qubits received from Charlie and report the result. Charlie compares the initial states of the decoy qubits and the result outcomes from Alice and Bob; he then checks the eavesdropping.[45,46]

4.3. Entity authentication phase

E1 Charlie randomly chooses only one communication member, Alice or Bob, to apply the Pauli operator on the $(2i-1)$-th or $2i$-th state of Eq. (10). If Charlie chooses Alice, then Alice applies the Pauli operator corresponding to the classical bit, k_i, to the $(2i-1)$-th state, such as in Eq. (7). If Charlie chooses Bob, then Bob applies the Pauli operator corresponding to the classical bit, k_i, to the $2i$-th state of Eq. (10). When classical bit k_i, which Alice and Bob share beforehand, is 10, the corresponding Pauli operator is $\mathrm{i}\sigma_y (= U_{10})$. If Charlie chooses Alice, then Alice applies U_{10} to the $(2i-1)$-th state $|\xi\rangle_{(2i-1)ABC}$ and Bob does not operate anything, as follows:

$$\begin{aligned} &|\xi'\rangle_{(2i-1)ABC} \otimes |\varepsilon'\rangle_{(2i)ABC} \\ &= [(U_{10} \otimes I \otimes I)|\xi\rangle_{(2i-1)ABC}] \otimes |\varepsilon\rangle_{(2i)ABC} \\ &= \left[\frac{1}{\sqrt{2}}(U_{10} \otimes I \otimes I)(|\Psi^+\rangle_{(2i-1)AB}|0\rangle_{(2i-1)C} \right. \\ &\quad \left. + |\Phi^+\rangle_{(2i-1)AB}|1\rangle_{(2i-1)C})\right] \\ &\quad \otimes \frac{1}{\sqrt{2}}(|\Phi^-\rangle_{(2i)AB}|0\rangle_{(2i)C} - |\Psi^+\rangle_{(2i)AB}|1\rangle_{(2i)C}) \\ &= \frac{1}{\sqrt{2}}(|\Phi^-\rangle_{(2i-1)AB}|0\rangle_{(2i-1)C} + |\Psi^-\rangle_{(2i-1)AB}|1\rangle_{(2i-1)C}) \\ &\quad \otimes \frac{1}{\sqrt{2}}(|\Phi^-\rangle_{(2i)AB}|0\rangle_{(2i)C} - |\Psi^+\rangle_{(2i)AB}|1\rangle_{(2i)C}). \end{aligned} \tag{11}$$

Through the public channel, Alice (or Bob) notifies Charlie that she (or he) has applied the Pauli operator.

E2 Charlie executes the σ_z basis measurement on the $(2i-1)$-th and $2i$-th qubit of his own qubit sequence. He notifies Alice and Bob only about the fact that he performed this action. After Charlie's measurement, the GHZ-like states of Eq. (11) collapse into $|\Phi^-\rangle_{(2i-1)AB}|\Phi^-\rangle_{(2i)AB}$, $|\Phi^-\rangle_{(2i-1)AB}|\Psi^+\rangle_{(2i)AB}$, $|\Psi^-\rangle_{(2i-1)AB}|\Phi^-\rangle_{(2i)AB}$, or $|\Psi^-\rangle_{(2i-1)AB}|\Psi^+\rangle_{(2i)AB}$ by a 25% probability, and Alice and Bob share one of the pairs of entangled states. For example, when the measurement outcomes are $|0\rangle_{(2i-1)c}$ and $|1\rangle_{(2i)c}$, Alice and Bob share $|\Phi^-\rangle_{(2i-1)AB} \otimes |\Psi^+\rangle_{(2i)AB}$. The shared entangled state $|\Phi^-\rangle_{(2i-1)AB} \otimes |\Psi^+\rangle_{(2i)AB}$ can be rearranged as follows:

$$\begin{aligned} &|\Phi^-\rangle_{(2i-1)AB} \otimes |\Psi^+\rangle_{(2i)AB} \\ &= \frac{1}{2}(|\Phi^+\rangle_{(2i-1)A(2i)A}|\Psi^-\rangle_{(2i-1)B(2i)B} \\ &\quad + |\Phi^-\rangle_{(2i-1)A(2i)A}|\Psi^+\rangle_{(2i-1)B(2i)B} \\ &\quad - |\Psi^+\rangle_{(2i-1)A(2i)A}|\Phi^-\rangle_{(2i-1)B(2i)B} \end{aligned}$$

$$-|\Psi^-\rangle_{(2i-1)A(2i)A}|\Phi^+\rangle_{(2i-1)B(2i)B}). \quad (12)$$

It is a superposed state of entangled states

$$|\Phi^+\rangle_{(2i-1)A(2i)A}|\Psi^-\rangle_{(2i-1)B(2i)B},$$
$$|\Phi^-\rangle_{(2i-1)A(2i)A}|\Psi^+\rangle_{(2i-1)B(2i)B},$$
$$|\Psi^+\rangle_{(2i-1)A(2i)A}|\Phi^-\rangle_{(2i-1)B(2i)B},$$
$$|\Psi^-\rangle_{(2i-1)A(2i)A}|\Phi^+\rangle_{(2i-1)B(2i)B}.$$

E3 By the Bell measurement performed by Alice and Bob, the entangled states between Alice and Bob $|\Phi^-\rangle_{(2i-1)AB}\otimes|\Psi^+\rangle_{(2i)AB}$ are collapsed into a product state of Alice's entangled state and Bob's entangled state, which is one of

$$|\Phi^+\rangle_{(2i-1)A(2i)A}|\Psi^-\rangle_{(2i-1)B(2i)B},$$
$$|\Phi^-\rangle_{(2i-1)A(2i)A}|\Psi^+\rangle_{(2i-1)B(2i)B},$$
$$|\Psi^+\rangle_{(2i-1)A(2i)A}|\Phi^-\rangle_{(2i-1)B(2i)B}$$

or $|\Psi^-\rangle_{(2i-1)A(2i)A}|\Phi^+\rangle_{(2i-1)B(2i)B}$. After this entanglement swapping, Alice and Bob announce their measurement outcomes, $a_{2i-1}a_{2i}$ and $b_{2i-1}b_{2i}$ ($a_j\&b_j\in\{0,1\}$, $j=2i-1$ or $2i$), as follows:

$$00:|\Phi^+\rangle=\frac{1}{\sqrt{2}}(|00\rangle+|11\rangle),$$
$$01:|\Phi^-\rangle=\frac{1}{\sqrt{2}}(|00\rangle-|11\rangle),$$
$$10:|\Psi^+\rangle=\frac{1}{\sqrt{2}}(|01\rangle+|10\rangle),$$
$$11:|\Psi^-\rangle=\frac{1}{\sqrt{2}}(|01\rangle-|10\rangle). \quad (13)$$

Charlie reveals the measurement outcome of classical bit $c_{2i-1}c_{2i}$ acquired in phase E2, where $c_{2i-1}c_{2i}\in\{00,01,10,11\}$. Both Alice and Bob confirm whether their classical bits, $a_{2i-1}a_{2i}$ and $b_{2i-1}b_{2i}$, correctly correspond to the revealed classical bit, $c_{2i-1}c_{2i}$, as shown in Table 4.

Table 4. k_i is a secret key shared between Alice and Bob. $a_{2i-1}a_{2i}$, $b_{2i-1}b_{2i}$, and $c_{2i-1}c_{2i}$ are measurement results produced by Alice, Bob, and Charlie, respectively. For example, if k_i is 10, $c_{2i-1}c_{2i}$ is 01, and $a_{2i-1}a_{2i}$ is 11, then $b_{2i-1}b_{2i}$ should be 00.

k_i : 00			k_i : 01			k_i : 10			k_i : 11		
00 Rev+−	00	11	00 ID+−	00	01	00 ID++	00	00	00 Rev++	00	10
	01	10		01	00		01	01		01	11
	10	01		10	11		10	10		10	00
	11	00		11	10		11	11		11	01
01 ID++	00	00	01 Rev++	00	10	01 Rev+−	00	11	01 ID+−	00	01
	01	01		01	11		01	10		01	10
	10	10		10	00		10	01		10	01
	11	11		11	01		11	00		11	00
10 ID+−	00	01	10 Rev+−	00	11	10 Rev++	00	10	10 ID++	00	00
	01	00		01	10		01	11		01	01
	10	11		10	01		10	00		10	10
	11	10		11	00		11	01		11	11
11 Rev++	00	10	11 ID++	00	00	11 ID+−	00	01	11 Rev+−	00	11
	01	11		01	01		01	00		01	10
	10	00		10	10		10	11		10	01
	11	11		11	11		11	10		11	00

In the example of phase E3, because the key, k_i, which Alice and Bob share, is 10, and Charlie's measurement result $c_{2i-1}c_{2i}$ is 01, the pair of measurement outcomes of Alice and Bob, $(a_{2i-1}a_{2i},b_{2i-1}b_{2i})$, must be one of the following four pairs: $\{(00,11),(01,10),(10,01),(11,00)\}$. If the calculated results $a_{2i-1}a_{2i}$ and $b_{2i-1}b_{2i}$ in phase E3 are consistent with Table 4, then the entities Alice and Bob are successfully authenticated. Otherwise, the entity authentication fails.

5. Security analysis

Two possible kinds of attack exist in our protocol. One is an internal attack in which communication users, Alice and Bob, try to verify each other without the controller, Charlie. The other is an external attack in which a third party, who is not a legitimate communication member, impersonates Alice, Bob, or Charlie. The internal attack is simulated as a double CNOT attack or entanglement attack;[15,46,47] the external attack is simulated as an intercept and resend attack.[12,23,44]

5.1. Internal attack: double CNOT attack (entanglement attack)

In explaining a double CNOT attack or entanglement attack, we suppose that, as a matter of convenience according to previous papers, the person who internally attacks Alice or Bob is Eve. The internal attacker, Eve, prepares ancilla states $|0\rangle_{(2i-1)E}\otimes|0\rangle_{(2i)E}$. The GHZ-like states $|\xi\rangle_{(2i-1)ABC}\otimes|\varepsilon\rangle_{(2i)ABC}$ and ancilla states $|0\rangle_{(2i-1)E}\otimes|0\rangle_{(2i)E}$ form a composite system, $|\Omega\rangle_{(2i-1)ABCE}\otimes|X\rangle_{(2i)ABCE}$, as follows:

$$|\Omega\rangle_{(2i-1)ABCE}\otimes|X\rangle_{(2i)ABCE}$$
$$=|\xi\rangle_{(2i-1)ABC}|0\rangle_{(2i-1)E}\otimes|\varepsilon\rangle_{(2i)ABC}|0\rangle_{(2i)E}$$

$$
\begin{aligned}
&= \frac{1}{2}(|0\rangle_A|0\rangle_B|1\rangle_C|0\rangle_E + |0\rangle_A|1\rangle_B|0\rangle_C|0\rangle_E \\
&\quad + |1\rangle_A|0\rangle_B|0\rangle_C|0\rangle_E + |1\rangle_A|1\rangle_B|1\rangle_C|0\rangle_E)_{(2i-1)} \\
&\quad \otimes \frac{1}{2}(|0\rangle_A|0\rangle_B|0\rangle_C|0\rangle_E - |1\rangle_A|0\rangle_B|1\rangle_C|0\rangle_E \\
&\quad - |0\rangle_A|1\rangle_B|1\rangle_C|0\rangle_E + |1\rangle_A|1\rangle_B|0\rangle_C|0\rangle_E)_{(2i)}. \qquad (14)
\end{aligned}
$$

Eve applies the CNOT operation C_{AE} and C_{BE}, where Alice's and Bob's states are control qubits, and Eve's state is a target qubit on the composite system $|\Omega\rangle_{(2i-1)ABCE} \otimes |X\rangle_{(2i)ABCE}$ of Eq. (16) as follows:

$$
\begin{aligned}
&|\Omega'\rangle_{(2i-1)ABCE} \otimes |X'\rangle_{(2i)ABCE} \\
&= C_{BE}C_{AE}|\Omega\rangle_{(2i-1)ABCE} \otimes C_{BE}C_{AE}|X\rangle_{(2i)ABCE} \\
&= C_{BE}C_{AE}|\xi\rangle_{(2i-1)ABC}|0\rangle_{(2i-1)E} \otimes C_{BE}C_{AE}|\varepsilon\rangle_{(2i)ABC}|0\rangle_{(2i)E} \\
&= \frac{1}{2}(|0\rangle_A|0\rangle_B|1\rangle_C|0\rangle_E + |0\rangle_A|1\rangle_B|0\rangle_C|1\rangle_E \\
&\quad + |1\rangle_A|0\rangle_B|0\rangle_C|1\rangle_E + |1\rangle_A|1\rangle_B|1\rangle_C|0\rangle_E)_{(2i-1)} \\
&\quad \otimes \frac{1}{2}(|0\rangle_A|0\rangle_B|0\rangle_C|0\rangle_E - |1\rangle_A|0\rangle_B|1\rangle_C|1\rangle_E \\
&\quad - |0\rangle_A|1\rangle_B|1\rangle_C|1\rangle_E + |1\rangle_A|1\rangle_B|0\rangle_C|0\rangle_E)_{(2i)}. \qquad (15)
\end{aligned}
$$

When Eve's measurement outcome of ancilla states and Charlie's measurement outcome in Eq. (15) are $e_{2i-1}e_{2i}$ and $c_{2i-1}c_{2i}$, respectively, $e_{2i-1}e_{2i}$ is identical to $(c_{2i-1} \oplus 1)(c_{2i})$, as shown in Table 5.

Table 5. Charlie's measurement outcome $c_{2i-1}c_{2i}$ and Eve's measurement outcome $e_{2i-1}e_{2i}$.

$c_{2i-1}c_{2i}$	$e_{2i-1}e_{2i} = (c_{2i-1} \oplus 1)(c_{2i})$
00	10
01	11
10	00
11	01

As a result, the internal attacker, Eve, can execute entity authentication without Charlie's assistance. Therefore, for the security of the protocol, in the preparation phase, Charlie sends Alice and Bob both N GHZ-like state(s) and N_C decoy qubits of

$$
|+\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}} \quad \text{or} \quad |+\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}}
$$

in random order.[45,46] After distributing N entangled states and N_C decoy qubits and completing the security check phase, the probability of detecting eavesdropping D is given as follows:

$$
\begin{aligned}
D &= d + d(1-d) + d(1-d)^2 + d(1-d)^3 + \cdots \\
&\quad + d(1-d)^{N_c-1} \\
&= \frac{d\{1-(1-d)^{N_c-1}\}}{1-(1-d)} = 1-(1-d)^{N_c-1}, \qquad (16)
\end{aligned}
$$

where d is the probability of detecting eavesdropping by checking one decoy qubit. If Charlie increases the number of decoy qubits N_C for the security of the communication channel, then the probability D of detecting Eve's intervention would be close to unity regardless of the value of d.

5.2. External attack: intercept and resend attack and Eve's impersonation

The external attacker, Eve, can either intercept two pairs of qubits, which are transmitted to Alice and Bob, and send two pairs of another GHZ-like state prepared as in Fig. 5(a), or intercept one pair of qubits, which are transmitted to Alice or Bob, and send a Bell state prepared as in Fig. 5(b). Likewise, with the intervention of Eve, the communication members can find, just by comparing the measurement outcome before entity authentication phase, whether there is an external attacker, Eve, since there is no correlation in the measurement outcome of the qubit which Alice, Bob, and Charlie, respectively, own. The probability of detecting Eve's existence is $1-(1/4)^n$, where n is the number of GHZ-like states.

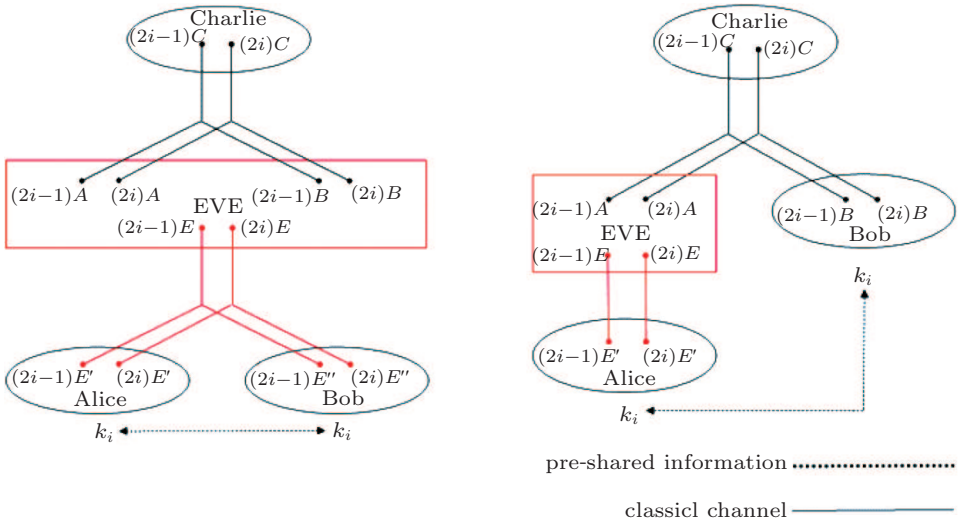


Fig. 5. (color online) Schematic representation of an intercept and resend attack.

If n is big enough, then the probability of detecting Eve's existence approaches to unity.[12,23,44] Furthermore, we use the decoy qubits to prevent both internal and external attack. The entangled state's correlation check method and the decoy qubit insert method guarantee the security of the communication channel.

6. Discussion and summary

The controlled mutual quantum entity authentication protocol that we proposed is adequate for use in a quantum network system in which no quantum communication line exists between two users, Alice and Bob. The communication line between two users is established through the transmission of a GHZ-like state by TC (or TTP), Charlie. TC performs only two von Neumann measurements to control the authentication process using the GHZ-like state, and the two users execute entanglement swapping, which makes mutual entity authentication possible. Also, like our protocol to build a quantum network system, there are a variety of quantum protocols which teleport quantum information or confirm pre-shared classical information. We compared these quantum protocols with our protocol in Table 6. Especially, Deng *et al.*'s controlled-quantum teleportation[35] which uses GHZ states to build a quantum network and teleports an unknown two-particle state by the help of an agent. Their controlled-quantum teleportation protocol can be applied to quantum secret sharing protocols,[35] and there are many other similar quantum secret sharing protocols[38–41]. If Deng *et al.*'s controlled-quantum teleportation replaces an unknown two-particle state with pre-shared secret information, then their protocol is similar to our entity authentication protocol. However, a controller in our protocol performs von Neumann measurement instead of Bell measurement. By the help of a controller, a mutual authentication of a prover and a verifier is possible in our protocol.

Table 6. Comparison of quantum protocols based on quantum network system.

		C-QT[35]	QSS based on C-QT[35]	QI[12]	RSP of a single particle state[44]	Our protocol
Source of quantum	three-particle state	2 GHZ states	2 GHZ states	None	2 GHZ states	2 GHZ states
	two-particle state	1 unknown two-particle state	1 Bell state	2 Bell states	none	none
	single-particle state	none	none	1 single particle state	none	none
Bell measurement		3 times	3 times	2 times	0 times	2 times
Two-dimensional projective Measurement		0 times	0 times	0 times	1 times	0 times
von Neumann measurement		0 times	0 times	0 time	2 times	2 times

For mutual authentication, two users must know the measurement outcome of TC (of TTP) in addition to the shared secret information. This is because the measurement outcome and its corresponding entangled states are completely random. In our protocol, the security checking process using the decoy qubit can prevent the double CNOT attack, which is the primary attack attempted by an adversary to obtain the measurement result of TC.

To access the quantum network system, the user must present his or her ID and corresponding password, which can be identified by TC. In our protocol, the secret key, k_i, plays the role of the password, which is shared in advance between users. The GHZ-like state in our protocol is analogous to the login webpage of a financial company or portal service. Anyone can participate in the authentication phase with the transmitted entangled states from TC in our protocol, just as anyone can access a login webpage—but no one logs in without a legitimate ID and password.

References

[1] Menezes A J, von Oorschot P C and Vantone S A 1996 *Handbook of Applied Cryptography* (Boca Raton: CRC Press)

[2] Schneier B 1995 *Applied Cryptography* (2nd edn.) (Wiley)

[3] Stinson D R 2005 *Cryptography: Theory and Practice* (3rd edn.) (Boca Raton: CRC Press)

[4] Forouzan B A 2008 *Cryptography and Network Security* (International Edition) (New York: McGraw Hill)

[5] *ISO/IEC* 9798-1 2010 *Information Technology–Security Techniques–Entity Authentication–Part 1: General*

[6] Bennett C H and Brassard G 1984 *Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing*, Bangalore, India, p. 175

[7] DuŜek M, Haderka O, Hendrych M and Mayska R 1999 *Phys. Rev. A* **60** 149

[8] Ljunggren D, Bourennane M and Karlsson A 2000 *Phys. Rev. A* **62** 022305

[9] Mihara T 2002 *Phys. Rev. A* **65** 052326

[10] Zhang Z S, Zeng G H, Zhou N R and Xiong J 2006 *Phys. Lett. A* **356** 199

[11] Huang P, Zhu J, Lu Y and Zeng G H 2011 *Int. J. Quantum Inf.* **9** 701

[12] Zhou N, Zeng G, Zeng W and Zhu F 2005 *Opt. Commun.* **254** 380

[13] Wang J, Zhang Q and Tang C J 2006 *Chin. Phys. Lett.* **23** 2360

[14] Yang Y G, Wen Q Y and Zhang X 2008 *Sci. China Ser. G, Phys. Astron.* **51** 321

[15] Yang Y G and Wen Q Y 2009 *Chin. Phys. B* **18** 3233

[16] Yang Y G, Wang H Y, Jin X and Zhang H 2013 *Int. J. Theor. Phys.* **52** 524

[17] Deng F G and Long G L 2004 *Phys. Rev. A* **70** 012311

[18] Nguyen B A 2004 *Phys. Lett. A* **328** 6

[19] Deng F G, Zhou H Y and Long G L 2005 *Phys. Lett. A* **337** 329

[20] Zhu A D, Xia Y, Fan Q G and Zhang S 2006 *Phys. Rev. A* **73** 022338

[21] Deng F G, Li X H, Li C Y, Zhou P and Zhou H Y 2006 *Phys. Lett. A* **359** 359
[22] Man Z X and Xia Y J 2006 *Chin. Phys. Lett.* **23** 1680
[23] Hong C H, Lim J I, Kim J I and Yang H J 2010 *J. Korean. Phys. Soc.* **56** 1733
[24] Gu B, Huang Y G, Fang X and Chen Y L 2011 *Commun. Theor. Phys.* **56** 659
[25] Zha X W, Zou Z C, Qi J X and Song H Y 2013 *Int. J. Theor. Phys.* **52** 1740
[26] Li Y H, Li X L, Sang M H, Nie Y Y and Wang Z S 2013 *Quantum. Inf. Process.* **12** 3835
[27] Yan L L, Chang Y and Zhang S B 2013 *Chin. Phys. Lett.* **30** 090301
[28] Heo J, Hong C H, Lim J I and Yang H J 2015 *Int. J. Theor. Phys.* 54 2261
[29] Hong C H, Heo J, Khym G L, Lim J I, Hong S K and Yang H J 2010 *Opt. Commun.* **283** 2644
[30] Hong C H, Heo J, Lim J I and Yang H J 2012 *Chin. Phys. Lett.* **29** 050303
[31] Hong C H, Heo J, Lim J I and Yang H J 2012 *J. Korean Phys. Soc.* **61** 1
[32] Hong C H, Heo J, Lim J I and Yang H J 2014 *Chin. Phys. B* **23** 090309
[33] Yoon C S, Kang M S, Lim J I and Yang H J 2015 *Phys. Scr.* **90** 015103
[34] Kang M S, Hong C H, Heo J, Lim J I and Yang H J 2015 *Int. J. Theor. Phys.* **54** 614
[35] Deng F G, Li C Y, Li Y S, Zhou H Y and Wang Y 2005 *Phys. Rev. A* **72** 022338
[36] Gao T, Yan F L and Wang Z X 2005 *Chin. Phys.* **14** 893
[37] Yang K, Huang L, Yang W and Song F 2009 *Int. J. Theor. Phys.* **48** 516
[38] Xiao L, Long G L, Deng F G and Pan J W 2004 *Phys. Rev. A* **69** 052307
[39] Li X H, Zhou P, Li C Y, Zhou H Y and Deng F G 2006 *J. Phys. B: At. Mol. Opt. Phys.* **39** 1975
[40] Deng F G, Zhou P, Li X H, Li C Y and Zhou H Y 2006 *Chin. Phys. Lett.* **23** 1084
[41] Hsieh C R, Tasi C W and Hwang T 2010 *Commun. Theor. Phys.* **54** 1019
[42] Kao S H and Hwang T 2013 *Chin. Phys. B* **22** 060308
[43] Dong Li, Xiu X M, Gao Y J, Ren Y P and Liu H W 2011 *Opt. Commun.* **284** 905
[44] Zhou N R, Cheng H L, Tao X Y and Gong L H 2014 *Quantum Inf. Process* **13** 513
[45] Li C Y, Zhou H Y, Wang Y and Deng F G 2005 *Chin. Phys. Lett.* **22** 1049
[46] Li C Y, Li X H, Deng F G, Zhou P, Liang Y J and Zhou H Y 2006 *Chin. Phys. Lett.* **23** 2896
[47] Li W, Fan M Y and Wang G W 2012 *Chin. Phys. B* **21** 120305
[48] Bennett C H 1992 *Phys. Rev. Lett.* **68** 3121
[49] Lo H K and Chau H F 1999 *Science* **283** 2050
[50] Shor P W and Preskill J 2000 *Phys. Rev. Lett.* **85** 441
[51] Long G L and Liu X S 2002 *Phys. Rev. A* **65** 032302
[52] Deng F D, Long G L and Liu X S 2003 *Phys. Rev. A* **68** 042317
[53] Deng F D and Long G L 2004 *Phys. Rev. A* **69** 052319
[54] Wang C, Deng F D, Li Y S, Liu X S and Long G L 2005 *Phys. Rev. A* **71** 044305
[55] Gu B, Zhang C Y, Cheng G S and Huang Y G 2011 *Sci. Chin: Phys. Mech. Astron.* **54** 942
[56] Gu B, Huang Y G, Fang X and Zhang C Y 2011 *Chin. Phys. B* **20** 100309
[57] Gu B, Huang Y G, Fang X and Chen Y L 2013 *Int. J. Theor. Phys.* **52** 4461
[58] Chang Y, Xu C X, Zhang S B and Yan L L 2013 *Chin. Sci. Bull.* **58** 4571