Quantum Inf Process (2018) 17:159
https://doi.org/10.1007/s11128-018-1927-5

Controlled mutual quantum entity authentication with an untrusted third party

Min-Sung Kang[1] · Jino Heo[2] · Chang-Ho Hong[3] · Hyung-Jin Yang[4,5] · Sang-Wook Han[1] · Sung Moon[1]

Received: 14 October 2017 / Accepted: 8 May 2018 / Published online: 18 May 2018

Abstract We propose a quantum control entity mutual authentication protocol that can be executed in environments involving an untrusted third party. In general, the third party, referred to as Charlie, can be an entity such as a telephone company, server, financial company, or login webpage for a portal service. Most communication protocols controlled by third parties are vulnerable to internal attacks. In this study, we present two solutions that make use of an entanglement correlation checking method and random numbers against an internal attack by an untrusted third party.

Keywords Quantum entity authentication · GHZ-like state · Untrusted third party · Internal attack

1 Introduction

Various quantum communication protocols, such as quantum key distribution(QKD) [1–3], measurement-device-independent QKD [4–6], controlled quantum teleportation [7–12], quantum secret sharing [13–22], controlled direct communication

✉ Sang-Wook Han
swhan@kist.re.kr

1 Center for Quantum Information, Korea Institute of Science and Technology (KIST), Seoul 02792, Republic of Korea

2 School of Information and Communication Engineering, Chungbuk National University, Chungdae-ro 1, Seowon-Gu, Cheongju, Republic of Korea

3 National Security Research Institute, P. O. Box 1, Yuseong, Daejeon 34188, Republic of Korea

4 Graduate School of Information Security, Korea University, Anam 5-ga, Sungbuk-gu, Seoul, Republic of Korea

5 Department of Physics, Korea University, Sejong 339-700, Republic of Korea

[23–30], remote state preparation [31–33], quantum private comparison [34], quantum steganography [35], and quantum key management [36] can be implemented on quantum networks [37–46]. All these protocols are based on an important assumption that a trusted third party is operating the quantum network. However, from the perspective of information security, a trusted third party does not exist, and there is a need for a quantum communication protocol that takes this into consideration. Furthermore, another topic of interest in the field of information security is the security of cloud services; thus, cloud services security is also being studied considering safety from third parties that provide such services. For example, in the case of a cloud service, user information is stored on a central server operated by a third party; therefore, the stored information can be leaked or altered by the third party. Blind quantum computation [47, 48] and homomorphic encryption [49, 50] are the methods used to prevent such leaks and alterations in cloud service.

In a previous study, we proposed a controlled mutual quantum entity authentication protocol [51] by which two communicators, referred to here as Alice and Bob, authenticate each other using entanglement swapping and under the control of a third party, Charlie, in a quantum network system established using a sequence of Greenberger–Horne–Zeilinger (GHZ)-like states. However, as mentioned previously, the assumption that Charlie is a trustworthy third party is not practical [52–54]. In this study, we present a method to ensure the security of our proposed protocol using an entanglement correlation check and random numbers to address the possibility that Charlie is an untrusted third party.

2 Brief review of controlled mutual quantum entity authentication

In this section, we outline our controlled mutual quantum entity authentication protocol [51]. Let us suppose that two communicators, Alice and Bob, want to authenticate each other in a quantum network created by the controller Charlie. This protocol consists of preparation, security checking, and entity authentication phases, which are discussed below.

2.1 Preparation phase

P1 Alice and Bob pre-share a secret key sequence $K_{AB} = (k_1, k_2, \ldots k_N)$ .The sequence $K_{AB} = (k_1, k_2, \ldots k_N)$ is of $2N$ bits; the elements are defined as $k_i \in \{00, 01, 10, 11\}$, and secret key k_i corresponds to the Pauli operator $U_{k_i} \in \left\{I, \sigma_x, i\sigma_y, \sigma_z\right\}$. The subscript AB represents that Alice and Bob shared the key

P2 A third party, Charlie, prepares the qubit sequence $(|\xi\rangle_1, |\xi\rangle_2, \ldots, |\xi\rangle_N)$ consisting of N GHZ-like states as follows:

$$|\xi\rangle_{(2i-1)123} \otimes |\xi\rangle_{(2i)123} = \frac{1}{\sqrt{2}}\left(\left|\Psi^+\right\rangle_{(2i-1)12}|0\rangle_{(2i-1)3} + \left|\Phi^+\right\rangle_{(2i-1)12}|1\rangle_{(2i-1)3}\right) \otimes \frac{1}{\sqrt{2}}\left(\left|\Phi^-\right\rangle_{(2i)12}|0\rangle_{(2i)3} - \left|\Psi^+\right\rangle_{(2i)12}|1\rangle_{(2i)3}\right) \quad (1)$$

The subscripts $(2i-1)$ and $(2i)$ refer to the odd-numbered qubits and even-numbered qubits, respectively, in the qubit sequence. In addition, the subscript 1, 2, or 3 indicates the order in the GHZ-like state.

P3 Charlie sends the first qubit to Alice, the second qubit to Bob, and retains the third qubit. He announces these facts to Alice and Bob. After Charlie's actions, the qubits are given as follows:

$$|\xi\rangle_{(2i-1)ABC} \otimes |\xi\rangle_{(2i)ABC} = \frac{1}{\sqrt{2}}\left(|\Psi^+\rangle_{(2i-1)AB}|0\rangle_{(2i-1)C} + |\Phi^+\rangle_{(2i-1)AB}|1\rangle_{(2i-1)C}\right) \otimes \frac{1}{\sqrt{2}}\left(|\Phi^-\rangle_{(2i)AB}|0\rangle_{(2i)C} - |\Psi^+\rangle_{(2i)AB}|1\rangle_{(2i)C}\right) \quad (2)$$

The subscript A, B, or C represents the owner of a particular qubit. While transmitting N GHZ-like states to Alice and Bob, Charlie randomly inserts N_C decoy qubits $|x+\rangle$, $|x-\rangle$ to detect eavesdropping [22, 34–36].

2.2 Security checking phase

S1 After confirming that Alice and Bob have safely received the qubit sequence, Charlie reveals the location of the decoy qubits [22, 34–36].

S2 Alice and Bob execute σ_x-basis measurements only on the decoy qubits received from Charlie and then report the results to Charlie. Charlie compares the initial states of the decoy qubits and the results reported by Alice and Bob. In effect, Charlie checks for eavesdropping [22, 34–36].

2.3 Entity authentication phase

E1 Charlie randomly selects one communication member, Alice or Bob, to apply the Pauli operation, which corresponds to the pre-shared key k_i, for the qubit $A_{(2i-1)}$ or $B_{(2i)}$ in Eq. (2).

E2 Charlie executes the σ_z-basis measurement on the qubits $\{C_{(2i-1)}, C_{(2i)}\}$ in Eq. (11) in Ref. [51]. And his measurement outcomes are $c_{2i-1}c_{2i}$, where $c_{2i-1}c_{2i} \in \{00, 01, 10, 11\}$. After Charlie's measurement, the GHZ-like states of Eq. (11) in Ref. [51] 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 $|\Psi^-\rangle_{(2i-1)AB}|\Psi^+\rangle_{(2i)AB}$ with a 25% probability, and Alice and Bob share one of the pairs of the entangled states.

E3 Alice and Bob execute the Bell-basis measurements on the qubits, $\left\{A_{(2i-1)}, A_{(2i)}\right\}$ and $\left\{B_{(2i-1)}, B_{(2i)}\right\}$, respectively; this is called entanglement swapping [36, 55, 56]. Then, they exchange their measurement outcomes, $a_{2i-1}a_{2i}$ and $b_{2i-1}b_{2i}(a_j \ \& \ b_j \in \{0, 1\}, \ j = 2i-1 \text{ or } 2i)$.

E4 Charlie reveals the measurement outcomes of the classical bit $c_{2i-1}c_{2i}$ acquired in phase E2. Then, 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 in [51].

3 Cryptanalysis of controlled mutual quantum entity authentication

Cryptographically, schemes without a third party are ideal; however, the use of trusted third parties in various cryptographic schemes is unavoidable to ensure efficiency and security. Nevertheless, as Ingemarsson and Simmons indicate [53, 54], anyone involved in cryptographic communication in commercial or international applications cannot be trusted. This deduction also applies to quantum communication protocols, and there are a variety of related cases involving untrustworthy communication elements [22, 36]. In particular, Gao and Wang showed that a security loophole exists in this protocol when the controller Charlie cannot be trusted [52]; in addition, they described how an untrusted controller Charlie can obtain legitimate users' authentication keys without introducing any errors in the protocol. Their procedure is described as follows.

Step 1 In phase P2, the controller Charlie executes sequential σ_z-basis measurements on qubits $\{3_{(2i-1)}, 3_{(2i)}\}$ of Eq. (1) and Bell-state measurements on qubits $\{1_{(2i-1)}, 1_{(2i)}\}$and $\{2_{(2i-1)}, 2_{(2i)}\}$ of Eq. (1), instead of sharing the GHZ-like states $|\xi\rangle_{(2i-1)123} \otimes |\xi\rangle_{(2i)123}$ of Eq. (1) with Alice and Bob. For example, when the σ_z-basis measurement outcomes are $|0\rangle_{(2i-1)3}$ and $|1\rangle_{(2i)3}$, the GHZ-like states of Eq. (1) collapse into $|\Psi^+\rangle_{(2i-1)12}|\Psi^+\rangle_{(2i)12}$, as follows:

$$|\Psi^+\rangle_{(2i-1)12}\,|\Psi^+\rangle_{(2i)12} = \frac{1}{2}\Big(|\Phi^+\rangle_{(2i-1)1(2i)1}\,|\Phi^+\rangle_{(2i-1)2(2i)2} + |\Phi^-\rangle_{(2i-1)1(2i)1}\,|\Phi^-\rangle_{(2i-1)2(2i)2} + |\Psi^+\rangle_{(2i-1)1(2i)1}\,|\Psi^+\rangle_{(2i-1)2(2i)2} + |\Psi^-\rangle_{(2i-1)1(2i)1}\,|\Psi^-\rangle_{(2i-1)2(2i)2}\Big). \tag{3}$$

In addition, if Charlie performs Bell-state measurements on qubits $\{1_{(2i-1)}, 1_{(2i)}\}$and $\{2_{(2i-1)}, 2_{(2i)}\}$ of Eq. (3), he can obtain measurement outcomes $(1_{2i-1}1_{2i}, 2_{2i-1}2_{2i})$ as:

$$\begin{aligned}(00,00):&\ |\Phi^+\rangle_{(2i-1)1(2i)1}\,|\Phi^+\rangle_{(2i-1)2(2i)2},\\ (01,01):&\ |\Phi^-\rangle_{(2i-1)1(2i)1}\,|\Phi^-\rangle_{(2i-1)2(2i)2},\\ (10,10):&\ |\Psi^+\rangle_{(2i-1)1(2i)1}\,|\Psi^+\rangle_{(2i-1)2(2i)2},\\ \text{or } (11,11):&\ |\Psi^-\rangle_{(2i-1)1(2i)1}\,|\Psi^-\rangle_{(2i-1)2(2i)2}.\end{aligned} \tag{4}$$

Table 1 represents all the outcomes corresponding to these measurements by Charlie.

Step 2 Charlie transmits the Bell states that correspond to the outcomes of Bell-state measurements to Alice and Bob. Here, Alice and Bob cannot detect Charlie's

Table 1 Measurement outcomes $3_{(2i-1)}3_{(2i)}$, $1_{(2i-1)}1_{(2i)}$, and $2_{(2i-1)}2_{(2i)}$ corresponding to the σ_z-basis and Bell-state measurements by Charlie

σ_z-basis measurements outcomes	Bell-state measurement outcomes	
$3_{(2i-1)}3_{(2i)}$	$1_{(2i-1)}1_{(2i)}$	$2_{(2i-1)}2_{(2i)}$
$00{:}\|0\rangle_{(2i-1)3}\|0\rangle_{(2i)3}$	$00{:}\|\Phi^+\rangle_{(2i-1)1(2i)1}$	$11{:}\|\Psi^-\rangle_{(2i-1)2(2i)2}$
	$01{:}\|\Phi^-\rangle_{(2i-1)1(2i)1}$	$10{:}\|\Psi^+\rangle_{(2i-1)2(2i)2}$
	$10{:}\|\Psi^+\rangle_{(2i-1)1(2i)1}$	$01{:}\|\Phi^-\rangle_{(2i-1)2(2i)2}$
	$11{:}\|\Psi^-\rangle_{(2i-1)1(2i)1}$	$00{:}\|\Phi^+\rangle_{(2i-1)2(2i)2}$
$01{:}\|0\rangle_{(2i-1)3}\|1\rangle_{(2i)3}$	$00{:}\|\Phi^+\rangle_{(2i-1)1(2i)1}$	$00{:}\|\Phi^+\rangle_{(2i-1)2(2i)2}$
	$01{:}\|\Phi^-\rangle_{(2i-1)1(2i)1}$	$01{:}\|\Phi^-\rangle_{(2i-1)2(2i)2}$
	$10{:}\|\Psi^+\rangle_{(2i-1)1(2i)1}$	$10{:}\|\Psi^+\rangle_{(2i-1)2(2i)2}$
	$11{:}\|\Psi^-\rangle_{(2i-1)1(2i)1}$	$11{:}\|\Psi^-\rangle_{(2i-1)2(2i)2}$
$10{:}\|1\rangle_{(2i-1)3}\|0\rangle_{(2i)3}$	$00{:}\|\Phi^+\rangle_{(2i-1)1(2i)1}$	$01{:}\|\Phi^-\rangle_{(2i-1)2(2i)2}$
	$01{:}\|\Phi^-\rangle_{(2i-1)1(2i)1}$	$00{:}\|\Phi^+\rangle_{(2i-1)2(2i)2}$
	$10{:}\|\Psi^+\rangle_{(2i-1)1(2i)1}$	$11{:}\|\Psi^-\rangle_{(2i-1)2(2i)2}$
	$11{:}\|\Psi^-\rangle_{(2i-1)1(2i)1}$	$10{:}\|\Psi^+\rangle_{(2i-1)2(2i)2}$
$11{:}\|1\rangle_{(2i-1)3}\|1\rangle_{(2i)3}$	$00{:}\|\Phi^+\rangle_{(2i-1)1(2i)1}$	$10{:}\|\Psi^+\rangle_{(2i-1)2(2i)2}$
	$01{:}\|\Phi^-\rangle_{(2i-1)1(2i)1}$	$11{:}\|\Psi^-\rangle_{(2i-1)2(2i)2}$
	$10{:}\|\Psi^+\rangle_{(2i-1)1(2i)1}$	$00{:}\|\Phi^+\rangle_{(2i-1)2(2i)2}$
	$11{:}\|\Psi^-\rangle_{(2i-1)1(2i)1}$	$01{:}\|\Phi^-\rangle_{(2i-1)2(2i)2}$

deception of using decoy qubits. Continuing with the example of Step 1, the Bell states that Alice and Bob receive from Charlie are given as follows:

$$\begin{aligned} &\left|\Phi^+\right\rangle_{(2i-1)A(2i)A}\left|\Phi^+\right\rangle_{(2i-1)B(2i)B},\\ &\left|\Phi^-\right\rangle_{(2i-1)A(2i)A}\left|\Phi^-\right\rangle_{(2i-1)B(2i)B},\\ &\left|\Psi^+\right\rangle_{(2i-1)A(2i)A}\left|\Psi^+\right\rangle_{(2i-1)B(2i)B},\\ \text{or } &\left|\Psi^-\right\rangle_{(2i-1)A(2i)A}\left|\Psi^-\right\rangle_{(2i-1)B(2i)B}. \end{aligned} \tag{5}$$

Step 3 Charlie requires Alice or Bob to apply the Pauli operator corresponding to the secret key k_i. If the secret key k_i is 01 and Charlie selects Alice, then Alice applies the Pauli operator $i\sigma_y(=U_{10})$ to Bell states of Eq. (5), as follows:

$$\begin{aligned} \left|\Psi^-\right\rangle_{(2i-1)A(2i)A}\left|\Phi^+\right\rangle_{(2i-1)B(2i)B} &= \left[i\sigma_y\left|\Phi^+\right\rangle_{(2i-1)A(2i)A}\right]\left|\Phi^+\right\rangle_{(2i-1)B(2i)B},\\ \left|\Psi^+\right\rangle_{(2i-1)A(2i)A}\left|\Phi^-\right\rangle_{(2i-1)B(2i)B} &= \left[i\sigma_y\left|\Phi^-\right\rangle_{(2i-1)A(2i)A}\right]\left|\Phi^-\right\rangle_{(2i-1)B(2i)B},\\ \left|\Phi^-\right\rangle_{(2i-1)A(2i)A}\left|\Psi^+\right\rangle_{(2i-1)B(2i)B} &= \left[i\sigma_y\left|\Psi^+\right\rangle_{(2i-1)A(2i)A}\right]\left|\Psi^+\right\rangle_{(2i-1)B(2i)B},\\ \text{or } \left|\Phi^+\right\rangle_{(2i-1)A(2i)A}\left|\Psi^-\right\rangle_{(2i-1)B(2i)B} &= \left[i\sigma_y\left|\Psi^-\right\rangle_{(2i-1)A(2i)A}\right]\left|\Psi^-\right\rangle_{(2i-1)B(2i)B}. \end{aligned} \tag{6}$$

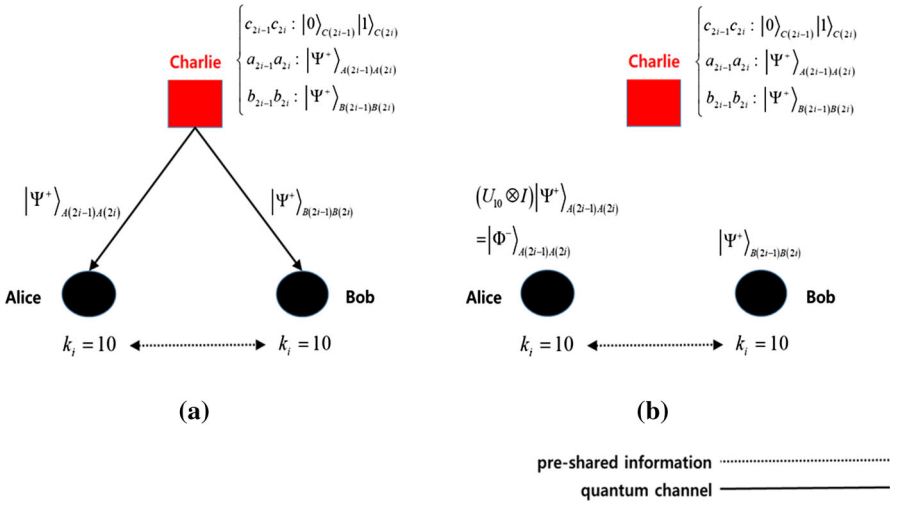

Fig. 1 Schematic illustration of untrusted controller Charlie's internal attack. **a** In phase P2, Charlie performs joint measurements and Bell-state measurements and then sends fake states $|\Psi^+\rangle_{A(2i-1)A(2i)}$ and $|\Psi^+\rangle_{B(2i-1)B(2i)}$ to Alice and Bob, respectively. **b** In phase E3, Charlie can estimate the secret key $k_i = 10$ using Bell measurement results from Alice and Bob

Step 4 Alice and Bob perform the Bell measurements on the Bell states of Eq. (6), and then they announce their measurement outcomes to Charlie. At this time, Charlie could identify the secret key k_i by knowing only one measurement outcome from Alice or Bob. Continuing with the example of Step 3, the measurement outcomes $(a_{2i-1}a_{2i}, b_{2i-1}b_{2i})$ of Alice and Bob are

$$\begin{aligned}
(11, 00) &: \left|\Psi^-\right\rangle_{(2i-1)A(2i)A} \left|\Phi^+\right\rangle_{(2i-1)B(2i)B}, \\
(10, 01) &: \left|\Psi^+\right\rangle_{(2i-1)A(2i)A} \left|\Phi^-\right\rangle_{(2i-1)B(2i)B}, \\
(01, 10) &: \left|\Phi^-\right\rangle_{(2i-1)A(2i)A} \left|\Psi^+\right\rangle_{(2i-1)B(2i)B}, \\
\text{or } (00, 11) &: \left|\Phi^+\right\rangle_{(2i-1)A(2i)A} \left|\Psi^-\right\rangle_{(2i-1)B(2i)B}.
\end{aligned} \tag{7}$$

Charlie can estimate that Alice's operator is $i\sigma_y (= U_{10})$ by comparing its measurement outcome $1_{2i-1}1_{2i}$ with Alice's measurement outcome $a_{2i-1}a_{2i}$. Based on this, Charlie can determine that the secret key is 10.

As a result, the controller Charlie can obtain the secret key shared between Alice and Bob using their measurement outcomes without disclosing his own measurement outcomes and without causing any errors. Figure 1 schematically illustrates the internal attack described above by the untrustworthy controller Charlie.

4 Security improvement of controlled mutual quantum entity authentication

4.1 Security improvement using entanglement correlation check

The security of various quantum communication protocols is ensured primarily by using decoy qubits [22, 34–36, 57–59] and entanglement correlation checking [34, 36, 60]. The insertion of decoy qubits is effective in detecting the involvement of malicious users in a quantum channel. Entanglement correlation checking is useful in determining whether quantum channel-based entangled states are well formed. In our controlled mutual quantum entity authentication protocol [51], we adopted decoy qubit insertion and entanglement correlation checking to ensure security. However, in this protocol, we did not consider the possibility of internal attack by a controller Charlie because we assumed that Charlie was a trustworthy third party. Therefore, we did not employ decoy qubit insertion or entanglement correlation checking to prevent an internal attack by Charlie. Gao et al. [52] indicated that, in real-world network communication, it is realistic to assume that the controller Charlie may be an untrustworthy third party. Therefore, an internal attack by the controller Charlie is possible because Alice and Bob do not check the correlation of the entangled state. To prevent this type of attack, we added a checking phase to confirm the correlation of the entangled state after phases S1 and S2. More specifically, Alice and Bob should select random states from among the sequence of N GHZ-like states $|\xi\rangle_{(2i-1)ABC} \otimes |\xi\rangle_{(2i)ABC}$ in Eq. (2) and perform $\sigma_z$or σ_x-basis measurements. For example, suppose Alice and Bob select the $(2j-1)$th state:

$$\begin{aligned} |\xi\rangle_{ABC(2j-1)} &= \frac{1}{\sqrt{2}}\left(\left|\Psi^{+}\right\rangle_{(2j-1)AB}|0\rangle_{(2j-1)C} + \left|\Phi^{+}\right\rangle_{(2j-1)AB}|1\rangle_{(2j-1)C}\right) \\ &= \frac{1}{\sqrt{2}}\left(|x+\rangle\,|x+\rangle\,|x+\rangle - |x-\rangle\,|x-\rangle\,|x-\rangle\right)_{(2j-1)ABC} \end{aligned} \tag{8}$$

to perform σ_x-basis measurements. Then, Alice and Bob inform Charlie of the location of the $(2j-1)$th state and the measurement basis σ_x. Charlie then performs the measurements in the same states as Alice and Bob and announces the measurement outcomes to them. Alice and Bob then announce their measurement outcomes to Charlie. In the case that Alice and Bob's measurement outcomes $a_{2j-1}b_{2j-1}$ are $++$: $|x+\rangle_{(2j-1)A}|x+\rangle_{(2j-1)B}$, then Charlie's measurement outcome c_{2j-1} would be $+$: $|x+\rangle_{(2j-1)C}$. If Charlie normally transmits GHZ-like states to Alice and Bob, the outcomes of Alice, Bob, and Charlie should be correlated. Alice and Bob should recognize Charlie's eavesdropping through the probability of $D = 1-(1-d)^{N_d}$, where d is the probability of detecting Charlie's eavesdropping by checking one GHZ-like state and N_d is the number of GHZ-like states used to detect Charlie's eavesdropping [61]. When N_d is sufficiently large, D approaches unity, and Alice and Bob can detect Charlie's eavesdropping. Table 2 lists all the measurement outcomes that can be obtained during the entanglement correlation check of the $(2j-1)^{\text{th}}$ state in Eq. (8). In the following lines, we provide a detailed explanation of how Alice and Bob can detect Charlie's eavesdropping mentioned earlier using the

Table 2 Measurement outcomes that can be caused by the entanglement correlation check of the $(2j-1)$th state in Eq. (8)

Measurement basis	c_{2j-1}	a_{2j-1}	b_{2j-1}
σ_z	$0{:}\|0\rangle_{(2j-1)C}$	$0{:}\|0\rangle_{(2j-1)A}$	$1{:}\|1\rangle_{(2j-1)B}$
		$1{:}\|1\rangle_{(2j-1)A}$	$0{:}\|0\rangle_{(2j-1)B}$
	$1{:}\|1\rangle_{(2j-1)C}$	$0{:}\|0\rangle_{(2j-1)A}$	$0{:}\|0\rangle_{(2j-1)B}$
		$1{:}\|1\rangle_{(2j-1)A}$	$1{:}\|1\rangle_{(2j-1)B}$
σ_x	$+{:}\|x+\rangle_{(2j-1)C}$	$+{:}\|x+\rangle_{(2j-1)A}$	$+{:}\|x+\rangle_{(2j-1)B}$
	$-{:}\|x-\rangle_{(2j-1)C}$	$-{:}\|x-\rangle_{(2j-1)A}$	$-{:}\|x-\rangle_{(2j-1)B}$

entanglement correlation check. Suppose Alice and Bob received the Bell states of Eq. (5) from Charlie as shown in Step 2 of Sect. 3, as follows.

$$\begin{aligned} &\left|\Phi^+\right\rangle_{(2i-1)A(2i)A}\left|\Phi^+\right\rangle_{(2i-1)B(2i)B},\\ &\left|\Phi^-\right\rangle_{(2i-1)A(2i)A}\left|\Phi^-\right\rangle_{(2i-1)B(2i)B},\\ &\left|\Psi^+\right\rangle_{(2i-1)A(2i)A}\left|\Psi^+\right\rangle_{(2i-1)B(2i)B},\\ \text{or}\ &\left|\Psi^-\right\rangle_{(2i-1)A(2i)A}\left|\Psi^-\right\rangle_{(2i-1)B(2i)B} \end{aligned} \tag{9}$$

Then, if Alice and Bob perform σ_x-basis measurements on the Bell state $\{A_{(2i-1)}, B_{(2i-1)}\}$ of Eq. (9), they can obtain measurement outcomes $(a_{2i-1}b_{2i-1})$, as follows.

$$\begin{aligned} (++) &: |x+\rangle_{(2i-1)A}\,|x+\rangle_{(2i-1)B}\\ (+-) &: |x+\rangle_{(2i-1)A}\,|x-\rangle_{(2i-1)B}\\ (-+) &: |x-\rangle_{(2i-1)A}\,|x+\rangle_{(2i-1)B}\\ \text{or}\ (--) &: |x-\rangle_{(2i-1)A}\,|x-\rangle_{(2i-1)B} \end{aligned} \tag{10}$$

Alice and Bob then inform Charlie of the $(2i-1)$th states and the measurement basis σ_x. At this time, Charlie should disclose the measurement outcome as if it had normally shared the entanglement state to make its attack successful. According to Table 2, the measurement outcomes $(+-) : |x+\rangle_{(2i-1)A}|x-\rangle_{(2i-1)B}$ and $(-+) : |x-\rangle_{(2i-1)A}|x+\rangle_{(2i-1)B}$ of Eq. (10) are only obtained by Charlie's attack. Furthermore, if the measurement outcome $(a_{2i-1}b_{2i-1})$ is $(++) : |x+\rangle_{(2i-1)A}|x+\rangle_{(2i-1)B}$, then Charlie must announce his measurement outcome $+ : |x+\rangle_{(2i\text{-}1)C}$. In contrast, if the measurement outcome $(a_{2i-1}b_{2i-1})$ is $(--) : |x-\rangle_{(2i-1)A}|x-\rangle_{(2i-1)B}$, then Charlie must announce his measurement outcome $- : |x-\rangle_{(2i-1)C}$. However, Charlie cannot predict Alice and Bob's measurement outcomes $(a_{2i-1}b_{2i-1})$, and therefore, Charlie always reveals the measurement outcomes incorrectly with a 50% probability. As a result, the probability that Charlie succeeds in its attack in such a case is 25%. More-

over, if they perform σ_z-basis measurements on the Bell state $\{A_{(2i-1)}, B_{(2i-1)}\}$ in Eq. (9), they can obtain measurement outcomes $(a_{2i-1}b_{2i-1})$, as follows.

$$\begin{aligned}(00) &: |0\rangle_{(2j-1)A}\,|0\rangle_{(2j-1)B}\,,\\ (01) &: |0\rangle_{(2j-1)A}\,|1\rangle_{(2j-1)B}\,,\\ (10) &: |1\rangle_{(2j-1)A}\,|0\rangle_{(2j-1)B}\,,\\ \text{or } (11) &: |1\rangle_{(2j-1)A}\,|1\rangle_{(2j-1)B}\end{aligned} \tag{11}$$

Alice and Bob then inform Charlie of the $(2i-1)$th states and the measurement basis σ_z. At this time, Charlie should disclose the measurement outcome as if it had normally shared the entanglement state to make his attack successful. According to Table 2, if the measurement outcome $(a_{2i-1}b_{2i-1})$ is $(01) : |0\rangle_{(2j-1)A}|1\rangle_{(2j-1)B}$ or $(10) : |1\rangle_{(2j-1)A}|0\rangle_{(2j-1)B}$, Charlie must announce his measurement outcome as $0{:}|0\rangle_{(2j-1)A}$. In addition, if the measurement outcome $(a_{2i-1}b_{2i-1})$ is $(00) : |0\rangle_{(2j-1)A}|0\rangle_{(2j-1)B}$ *or* $(11) : |1\rangle_{(2j-1)A}|1\rangle_{(2j-1)B}$, Charlie must announce his measurement outcome as $1{:}|1\rangle_{(2j-1)A}$. However, Charlie cannot predict Alice and Bob's measurement outcomes $(a_{2i-1}b_{2i-1})$; thus, Charlie fails the attack with a 50% probability.

4.2 Security improvement using random numbers

As mentioned above, the controller Charlie can predict the secret key from the measurement outcomes of Alice and Bob, without sharing his measurement outcomes with them. Therefore, if there is a method that prevents the controller Charlie from guessing the secret key, the security of our proposed protocol is ensured. The proposed method involves using a random number; the protocol that modifies the entity authentication phase is described as follows.

E1. (a) Alice and Bob prepare random numbers r_A and r_B, where $r_A, r_B \in \{00, 01, 10, 11\}$.

E1. (b) Charlie randomly selects only one communication member, Alice or Bob. If Charlie selects Alice, Alice applies the Pauli operator corresponding to the classical information $k'_i \oplus r_A = k_{(i)A}$ to the qubit $A_{(2i-1)}$. If Charlie selects Bob, Bob applies the Pauli operator corresponding to the classical bit $k'_i \oplus r_B = k_{(i)B}$ to the qubit $B_{(2i)}$. Here, $k'_i \left(= k_{(i)A} \oplus r_A \text{ or } k_{(i)B} \oplus r_B\right)$ is a pre-shared secret key between Alice and Bob in the preparation phase, $k_i \in \{00, 01, 10, 11\}$. For example, when $k'_i = 11$ and $r_A = 01$, Alice applies the Pauli operator $i\sigma_y \left(= U_{k'_i \oplus r_A}\right)$ to the qubit $A_{(2i-1)}$; this is performed as follows:

$$
\begin{aligned}
&\left(i\sigma_y \otimes I \otimes I\right) |\xi\rangle_{(2i-1)ABC} \otimes |\xi\rangle_{(2i)ABC} \\
&= \frac{1}{\sqrt{2}} \left(i\sigma_y \otimes I \otimes I\right) \left(\left|\Psi^+\right\rangle_{(2i-1)AB} |0\rangle_{(2i-1)C} + \left|\Phi^+\right\rangle_{(2i-1)AB} |1\rangle_{(2i-1)C} \right) \\
&\quad \otimes \frac{1}{\sqrt{2}} \left(\left|\Phi^-\right\rangle_{(2i)AB} |0\rangle_{(2i)C} - \left|\Psi^+\right\rangle_{(2i)AB} |1\rangle_{(2i)C} \right) \\
&= \frac{1}{\sqrt{2}} \left(\left|\Phi^-\right\rangle_{(2i-1)AB} |0\rangle_{(2i-1)C} + \left|\Psi^-\right\rangle_{(2i-1)AB} |1\rangle_{(2i-1)C} \right) \\
&\quad \otimes \frac{1}{\sqrt{2}} \left(\left|\Phi^-\right\rangle_{(2i)AB} |0\rangle_{(2i)C} - \left|\Psi^+\right\rangle_{(2i)AB} |1\rangle_{(2i)C} \right)
\end{aligned} \tag{12}
$$

As another example, when $k_i' = 11$and $r_B = 10$, Bob applies the Pauli operator $\sigma_x \left(= U_{k_i' \oplus r_B}\right)$ to the qubit $B_{(2i)}$; this is performed as follows:

$$
\begin{aligned}
&|\xi\rangle_{(2i-1)ABC} \otimes \left(I \otimes \sigma_x \otimes I\right) |\xi\rangle_{(2i)ABC} \\
&= \frac{1}{\sqrt{2}} \left(\left|\Psi^+\right\rangle_{(2i-1)AB} |0\rangle_{(2i-1)C} + \left|\Phi^+\right\rangle_{(2i-1)AB} |1\rangle_{(2i-1)C} \right) \\
&\quad \otimes \frac{1}{\sqrt{2}} \left(I \otimes \sigma_x \otimes I\right) \left(\left|\Phi^-\right\rangle_{(2i)AB} |0\rangle_{(2i)C} - \left|\Psi^+\right\rangle_{(2i)AB} |1\rangle_{(2i)C} \right) \\
&= \frac{1}{\sqrt{2}} \left(\left|\Psi^+\right\rangle_{(2i-1)AB} |0\rangle_{(2i-1)C} + \left|\Phi^+\right\rangle_{(2i-1)AB} |1\rangle_{(2i-1)C} \right) \\
&\quad \otimes \frac{1}{\sqrt{2}} \left(\left|\Psi^-\right\rangle_{(2i)AB} |0\rangle_{(2i)C} - \left|\Phi^+\right\rangle_{(2i)AB} |1\rangle_{(2i)C} \right)
\end{aligned} \tag{13}
$$

E2 Charlie executes the σ_z-basis measurement on the qubits $\{C_{(2i-1)}, C_{(2i)}\}$ in Eq. (12). And his measurement outcome is $c_{2i-1}c_{2i}$, where $c_{2i-1}c_{2i} \in \{00, 01, 10, 11\}$. After Charlie's measurement, the GHZ-like states of Eq. (12) collapse into

$$
\left|\Phi^-\right\rangle_{(2i-1)AB} \left|\Phi^-\right\rangle_{(2i)AB}, \ \left|\Phi^-\right\rangle_{(2i-1)AB} |\Psi^+\rangle_{(2i)AB}, \ \left|\Psi^-\right\rangle_{(2i-1)AB} \left|\Phi^-\right\rangle_{(2i)AB}, \text{ or } \left|\Psi^-\right\rangle_{(2i-1)AB} |\Psi^+\rangle_{(2i)AB} \tag{14}
$$

with a 25% probability, and Alice and Bob share one of the pairs of the entangled states. Continuing with the first example of E1. (b), when $c_{2i-1}c_{2i} = 01$, the GHZ-like states of Eq. (12) collapse into $|\Phi^-\rangle_{(2i-1)AB}|\Psi^+\rangle_{(2i)AB}$:

$$
\begin{aligned}
\left|\Phi^-\right\rangle_{(2i-1)AB} |\Psi^+\rangle_{(2i)AB} = \frac{1}{2} \Big(&\left|\Phi^+\right\rangle_{(2i-1)A(2i)A} |\Psi^-\rangle_{(2i-1)B(2i)B} + \left|\Phi^-\right\rangle_{(2i-1)A(2i)A} |\Psi^+\rangle_{(2i-1)B(2i)B} \\
&+ |\Psi^+\rangle_{(2i-1)A(2i)A} \left|\Phi^-\right\rangle_{(2i-1)B(2i)B} + \left|\Psi^-\right\rangle_{(2i-1)A(2i)A} |\Phi^+\rangle_{(2i-1)B(2i)B} \Big)
\end{aligned} \tag{15}
$$

And, continuing with the second example of E1. (b), when $c_{2i-1}c_{2i} = 01$, the GHZ-like states of Eq. (13 collapse into $|\Psi^+\rangle_{(2i-1)AB}|\Phi^+\rangle_{(2i)AB}$:

$$|\Psi^{+}\rangle_{(2i-1)AB}|\Phi^{+}\rangle_{(2i)AB} = \frac{1}{2}\left(|\Phi^{+}\rangle_{(2i-1)A(2i)A}|\Psi^{+}\rangle_{(2i-1)B(2i)B} + |\Phi^{-}\rangle_{(2i-1)A(2i)A}|\Psi^{-}\rangle_{(2i-1)B(2i)B} + |\Psi^{+}\rangle_{(2i-1)A(2i)A}|\Phi^{+}\rangle_{(2i-1)B(2i)B} + |\Psi^{-}\rangle_{(2i-1)A(2i)A}|\Phi^{-}\rangle_{(2i-1)B(2i)B}\right) \quad (16)$$

E3 Alice and Bob execute the Bell-basis measurements on the qubits $\{A_{(2i-1)}, A_{(2i)}\}$and $\{B_{(2i-1)}, B_{(2i)}\}$ of Eq. (13), respectively. Then, they exchange 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 $2i$). Continuing with the first example of E2, if Alice and Bob perform Bell-state measurement on $\{A_{(2i-1)}, A_{(2i)}\}$ and $\{B_{(2i-1)}, B_{(2i)}\}$ of Eq. (15), they can obtain measurement outcomes ($a_{2i-1}a_{2i}$, $b_{2i-1}b_{2i}$) as:

$$\begin{aligned}(00, 11) &: |\Phi^{+}\rangle_{(2i-1)A(2i)A}|\Psi^{-}\rangle_{(2i-1)B(2i)B},\\ (01, 10) &: |\Phi^{-}\rangle_{(2i-1)A(2i)A}|\Psi^{-}\rangle_{(2i-1)B(2i)B},\\ (01, 10) &: |\Psi^{-}\rangle_{(2i-1)A(2i)A}|\Phi^{-}\rangle_{(2i-1)B(2i)B},\\ \text{or } (11, 00) &: |\Psi^{-}\rangle_{(2i-1)A(2i)A}|\Phi^{+}\rangle_{(2i-1)B(2i)B}. \end{aligned} \quad (17)$$

Then, they exchange their measurement outcomes ($a_{2i-1}a_{2i}$, $b_{2i-1}b_{2i}$) in Eq. (17). And continuing with the second example of E2, if Alice and Bob perform Bell-state measurement on $\{A_{(2i-1)}, A_{(2i)}\}$ and $\{B_{(2i-1)}, B_{(2i)}\}$ of Eq. (16), they can obtain measurement outcomes ($a_{2i-1}a_{2i}$, $b_{2i-1}b_{2i}$) as:

$$\begin{aligned}(00, 10) &: |\Phi^{+}\rangle_{(2i-1)A(2i)A}|\Psi^{+}\rangle_{(2i-1)B(2i)B},\\ (01, 11) &: |\Phi^{-}\rangle_{(2i-1)A(2i)A}|\Psi^{-}\rangle_{(2i-1)B(2i)B},\\ (10, 00) &: |\Psi^{+}\rangle_{(2i-1)A(2i)A}|\Phi^{+}\rangle_{(2i-1)B(2i)B},\\ \text{or } (11, 01) &: |\Psi^{-}\rangle_{(2i-1)A(2i)A}|\Phi^{-}\rangle_{(2i-1)B(2i)B}. \end{aligned} \quad (18)$$

Then, they exchange their measurement outcomes ($a_{2i-1}a_{2i}$, $b_{2i-1}b_{2i}$) in Eq. (18).

E4. (a) Charlie reveals the measurement outcomes $c_{2i-1}c_{2i}$ acquired in Phase E2; then, Alice or Bob announces r_A or r_B to Charlie, respectively. Continuing with the first example of E3, Charlie and Alice announce $c_{2i-1}c_{2i} = 01$ and $r_A = 01$ to each other in turn. And, continuing with the second example of E3, Charlie and Bob announce $c_{2i-1}c_{2i} = 01$ and $r_B = 01$ to each other in turn.

E4. (b) Alice and Bob confirm whether their classical bits, $a_{2i-1}a_{2i}$, $b_{2i-1}b_{2i}$, and $c_{2i-1}c_{2i}$, correspond correctly to the classical bit $k_{(i)A} = k'_i \oplus r_A$ or $k_{(i)B} = k'_i \oplus r_B$, as presented in Table 4 in [51]. Continuing with the first example of E4. (a), if $k'_i = 11$, $a_{2i-1}a_{2i} = 11$, $b_{2i-1}b_{2i} = 00$, and $c_{2i-1}c_{2i} = 01$. $k_{(i)A} = k'_i \oplus r_A$ must then be 10. And Continuing with the first example of E4. (1) $k'_i = 11$, $a_{2i-1}a_{2i} = 11$, $b_{2i-1}b_{2i} = 01$, and $c_{2i-1}c_{2i} = 01$. $k_{(i)B} = k'_i \oplus r_B$ must then be 01.

Consequently, even if Charlie attempts an internal attack, he cannot estimate the pre-shared secret key k_i without knowing the random numbers r_A or r_B. Suppose Alice and Bob received the Bell states in Eq. (5) from Charlie as shown in Step 2 of Sect. 3.

When $k'_i = 11$ and $r_A = 01$, Alice applies the Pauli operator $i\sigma_y \left(= U_{k'_i \oplus r_A}\right)$ to the qubit $A_{(2i-1)}$ of in Eq. (5):

$$\begin{aligned}
\left|\Psi^-\right\rangle_{(2i-1)A(2i)A} \left|\Phi^+\right\rangle_{(2i-1)B(2i)B} &= \left[i\sigma_y \left|\Phi^+\right\rangle_{(2i-1)A(2i)A}\right] \left|\Phi^+\right\rangle_{(2i-1)B(2i)B}, \\
\left|\Psi^+\right\rangle_{(2i-1)A(2i)A} \left|\Phi^-\right\rangle_{(2i-1)B(2i)B} &= \left[i\sigma_y \left|\Phi^-\right\rangle_{(2i-1)A(2i)A}\right] \left|\Phi^-\right\rangle_{(2i-1)B(2i)B}, \\
\left|\Phi^-\right\rangle_{(2i-1)A(2i)A} \left|\Psi^+\right\rangle_{(2i-1)B(2i)B} &= \left[i\sigma_y \left|\Psi^+\right\rangle_{(2i-1)A(2i)A}\right] \left|\Psi^+\right\rangle_{(2i-1)B(2i)B}, \\
\text{or} \quad \left|\Phi^+\right\rangle_{(2i-1)A(2i)A} \left|\Psi^-\right\rangle_{(2i-1)B(2i)B} &= \left[i\sigma_y \left|\Psi^-\right\rangle_{(2i-1)A(2i)A}\right] \left|\Psi^-\right\rangle_{(2i-1)B(2i)B}.
\end{aligned} \tag{19}$$

If Alice and Bob perform Bell-state measurement on $\{A_{(2i-1)}, A_{(2i)}\}$ and $\{B_{(2i-1)}, B_{(2i)}\}$ of Eq. (19), they can obtain measurement outcomes $(a_{2i-1}a_{2i}, b_{2i-1}b_{2i})$ as:

$$\begin{aligned}
(11, 00) &: \left|\Psi^-\right\rangle_{(2i-1)A(2i)A} \left|\Phi^+\right\rangle_{(2i-1)B(2i)B}, \\
(10, 01) &: \left|\Psi^+\right\rangle_{(2i-1)A(2i)A} \left|\Phi^-\right\rangle_{(2i-1)B(2i)B}, \\
(01, 10) &: \left|\Phi^-\right\rangle_{(2i-1)A(2i)A} \left|\Psi^+\right\rangle_{(2i-1)B(2i)B}, \\
\text{or } (00, 11) &: \left|\Phi^+\right\rangle_{(2i-1)A(2i)A} \left|\Psi^-\right\rangle_{(2i-1)B(2i)B}.
\end{aligned} \tag{20}$$

Later, if Alice and Bob release the Bell measurements $a_{2i\text{-}1}a_{2i} = 11$ and $b_{2i\text{-}1}b_{2i} = 00$, Charlie gets to know the $k_{(i)A} = k'_i \oplus r_A = 10$. But Charlie cannot guess the secret key $k_{(i)A} = k'_i \oplus r_A = 11$, because he does not know the random numbers $r_A = 01$.

5 Conclusions

We proposed a secure controlled mutual quantum object authentication protocol that is viable even in an environment in which users cannot trust third party. Two schemes for ensuring the safety of the protocol are used: one is entanglement correlation checking, and the other is the use of random numbers. Entanglement correlation checking can be used to determine whether there is an abnormality in the quantum channel, while random numbers are used in the protocol to make it impossible for the untrusted controller to deduce the key directly. By applying these security protocols to a quantum network, we expect to prevent any malfeasance by an untrusted controller as well as an eavesdropper.

Acknowledgements This work was supported by the ICT R&D programs of MSIP/IITP (Grant No. B0101-16-1355), the KIST research program (Grant No. 2E27801). C.-H. Hong is supported by the ICT R&D program of MSIP/IITP [1711057505, Reliable crypto-system standards and core technology development for secure quantum key distribution network].

References

1. Bennett, C.H., Brassard, G.: Quantum cryptography: public-key distribution and coin tossing. In: IEEE International Conference on Computers Systems and Signal Processing, Bangalore, India, pp. 175–179. IEEE, New York (1984)
2. Ekert, A.K.: Quantum cryptography based on Bell theorem. Phys. Rev. Lett. **67**(6), 661–663 (1991)
3. Bennett, C.H.: Quantum cryptography using any two nonorthogonal states. Phys. Rev. Lett. **68**(21), 3121–3124 (1992)
4. Lo, H.-K., Curty, M., Qi, B.: Measurement-device-independent quantum key distribution. Phys. Rev. Lett. **108**, 130503 (2012)
5. Tang, Y.L., Yin, H.L., Chen, S.J., et al.: Measurement-device-independent quantum key distribution over 200 km. Phys. Rev. Lett. **114**, 069901 (2015)
6. He, J., Li, Q., Wu, C., Chan, W.H., Zhang, S.: Measurement-device-independent semiquantum key distribution. Int. J. Quantum Inf. **16**, 1850012 (2018)
7. Zhao, Z., Chen, Y.A., Zhang, A.N., Yang, T., Briegel, H.J., Pan, J.W.: Experimental demonstration of five-photon entanglement and open-destination teleportation. Nature **430**, 54–58 (2004)
8. Deng, F.G., Li, C.Y., Li, Y.S., Zhou, H.Y., Wang, Y.: Symmetric multiparty-controlled teleportation of an arbitrary two-particle entanglement. Phys. Rev. A **72**, 022338 (2005)
9. Gao, T., Yan, F.L., Wang, Z.X.: Controlled quantum teleportation and secure direct communication. Chin. Phys. **14**(5), 893–897 (2005)
10. Yang, K., Huang, L., Yang, W., Song, F.: Quantum teleportation via GHZ-like state. Int. J. Theor. Phys. **48**, 516–521 (2009)
11. Wang, X.W., Su, Y.H., Yang, G.J.: Controlled teleportation against uncooperation of part of supervisors. Quantum Inf. Process. **8**, 319–330 (2009)
12. Wang, T.Y., Wen, Q.Y.: Controlled quantum teleportation with Bell states. Chin. Phys. B **20**(4), 040307 (2011)
13. Hillery, M., Bužek, V., Berthiaume, A.: Quantum secret sharing. Phys. Rev. A **59**(3), 1829–1834 (1999)
14. Karlsson, A., Koashi, M., Imoto, N.: Quantum entanglement for secret sharing and secret splitting. Phys. Rev. A **59**(1), 162–168 (1999)
15. Xiao, L., Long, G.L., Deng, F.G., Pan, J.W.: Efficient multiparty quantum–secret–sharing schemes. Phys. Rev. A **69**, 052307 (2004)
16. Deng, F.G., Li, X.H., Li, C.Y., Zhou, P., Zhou, H.Y.: Multiparty quantum-state sharing of an arbitrary two-particle state with Einstein–Podolsky–Rosen pairs. Phys. Rev. A **72**, 044301 (2005)
17. Deng, F.G., Li, X.H., Zhou, H.Y.: Improving the security of multiparty quantum secret sharing against trojan horse attack. Phys. Rev. A **72**, 044302 (2005)
18. Li, X.H., Zhou, P., Li, C.Y., et al.: Efficient symmetric multiparty quantum state sharing of an arbitrary m-qubit state. J. Phys. B: At. Mol. Opt. Phys. **39**(8), 1975–1983 (2006)
19. Deng, F.G., Zhou, P., Li, X.H., Li, C.Y., Zhou, H.Y.: Efficient multiparty quantum secret sharing with Greenberger-Horne-Zeilinger States. Chin. Phys. Lett. **23**(5), 1084–1087 (2006)
20. Hsieh, C.R., Tsai, C.W., Hwang, T.: Quantum secret sharing using GHZ-like state. Commun. Theor. Phys. **54**(6), 1019–1022 (2010)
21. Chen, X.B., Niu, X.X., Zhou, X.J., Yang, Y.X.: Multi-party quantum secret sharing with the single-particle quantum state to encode the information. Quantum Inf. Process. **12**, 365–380 (2013)
22. Chen, X.B., Xu, G., Su, Y., Yang, Y.X.: Robust variations of secret sharing through noisy quantum channel. Quantum Inf. Comput. **14**(78), 589–607 (2014)
23. Man, Z.X., Zhang, Z.J., Li, Y.: Deterministic secure direct communication by using swapping quantum entanglement and local unitary operations. Chin. Phys. Lett. **22**(1), 18–21 (2005)
24. Gao, T., Yan, F.L., Wang, Z.X.: Deterministic secure direct communication using GHZ states and swapping quantum entanglement. J. Phys. A **38**, 5761 (2005)
25. Wang, C., Deng, F., Long, G.: Multi-step quantum secure direct communication using multi-particle Green-Horne-Zeilinger state. Opt. Commun. **253**, 15 (2005)
26. Lee, H., Lim, J., Yang, H.: Quantum direct communication with authentication. Phys. Rev. A **73**, 042305 (2006)
27. Jin, X.R., Ji, X., Zhang, Y.Q., Zhang, S., Hong, S.K., Yeon, K.H., Um, C.I.: Three-party quantum secure direct communication based on GHZ states. Phys. Lett. A **354**(1), 67–70 (2006)
28. Man, Z.-X., Xia, Y.-J., An, N.B.: Quantum secure direct communication by using GHZ states and entanglement swapping. J. Phys. B: At. Mol. Opt. Phys. **39**, 3855–3864 (2006)

29. Kao, S.H., Hwang, T.: Cryptanalysis and improvement of controlled secure direct communication. Chin. Phys. B **22**, 060308 (2013)
30. Dong, L., Xiu, X.M., Gao, Y.J., Ren, Y.P., Liu, H.W.: Controlled three-party communication using GHZ-like state and imperfect Bell-state measurement. Opt. Commun. **284**, 905–908 (2011)
31. Dai, H.Y., Chen, P.X., Zhang, M., Li, C.Z.: Classical communication cost and remote preparation of the four-particle GHZ class state. Phys. Lett. A **355**, 285–288 (2006)
32. Peng, J.Y., Luo, M.X., Mo, Z.W.: Joint remote state preparation of arbitrary two-particle states via GHZ-type states. Quantum Inf. Process. **12**, 2325–2342 (2013)
33. Zhou, N.R., Cheng, H.L., Tao, X.Y., Gong, L.H.: Three-party remote state preparation schemes based on entanglement. Quantum Inf. Process. **13**, 513 (2014)
34. Chen, X.-B., Dou, Z., Xu, G., Wang, C., Yang, Y.: A class of protocols for quantum private comparison based on the symmetry of states. Quantum Inf. Process. **13**, 85 (2014)
35. Wei, Z.H., Chen, X.B., Niu, X.X., et al.: The quantum steganography protocol via quantum noisy channels. Int. J. Theor. Phys. **54**(8), 2505–2515 (2015)
36. Xu, G., Chen, X.-B., Dou, Z., Yang, Y.-X., Li, Z.: A novel protocol for multiparty quantum key management. Quantum Inf. Process. **14**, 2959–2980 (2015)
37. Peev, M., Pacher, C., Alléaume, R., et al.: The SECOQC quantum key distribution network in Vienna. New J. Phys. **11**, 075001 (2009)
38. Sasaki, M., Fujiwara, M., Ishizuka, H., et al.: Field test of quantum key distribution in the Tokyo QKD network. Opt. Express **19**, 10387–10409 (2011)
39. Ursin, R., Tiefenbacher, F., Schmitt-Manderbach, T., et al.: Entanglement-based quantum communication over 144 km. Nat. Phys. **3**, 481–486 (2007)
40. Fröhlich, B., Dynes, J.F., Lucamarini, M., Sharpe, A.W., Yuan, Z., Shields, A.J.: A quantum access network. Nature **501**(7465), 69–72 (2013)
41. Tang, Y.-L., Yin, H.-L., Zhao, Q., et al.: Measurement-device-independent quantum key distribution over untrustful metropolitan network. Phys. Rev. X **6**, 011024 (2016)
42. Hong, C.H., Heo, J., Khym, G.L., Lim, J.I., Hong, S.K., Yang, H.J.: N quantum channels are sufficient for multi-user quantum key distribution protocol between n users. Opt. Commun. **283**, 2644 (2010)
43. Hong, C.H., Heo, J., Lim, J.I., Yang, H.J.: A quantum network system of QSS-QDC using χ-type entangled states. Chin. Phys. Lett. **29**, 050303 (2012)
44. Hong, C.H., Heo, J., Lim, J.I., Yang, H.J.: Multi-user quantum network system and quantum communication using χ-type entangled states. J. Korean. Phys. Soc. **61**, 1–5 (2012)
45. Hong, C.H., Heo, J., Lim, J.I., Yang, H.J.: Quantum secure direct communication network with hyper-entanglement. Chin. Phys. B **23**, 090309 (2014)
46. Li, J., Chen, X.B., Xu, G., et al.: Perfect quantum network coding independent of classical network solutions. IEEE Commun. Lett. **19**, 115–118 (2015)
47. Broadbent, A.J., Fitzsimons, F., Kashefi, E.: Universal blind quantum computation. In: Proceedings of the 50th Annual IEEE Symposium on Foundations of Computer Science, p. 517. IEEE Computer Society, Los Alamitos (2009)
48. Li, Q., Li, Z., Chan, W.H., Zhang, S., Liu, C.: Blind quantum computation with identity authentication. Phys. Lett. A **382**, 938 (2018)
49. Naehrig, M., Lauter, K., Vaikuntanathan, V.: Can homomorphic encryption be practical? In: Proceedings of the 3rd ACM Workshop on Cloud Computing Security, pp. 113–124 (2011)
50. Tebaa, M., El Hajji, S., El Ghazi, A.: Homomorphic encryption applied to the cloud computing security. Proc. World Congr. Eng. **1**, 4–6 (2012)
51. Kang, M.S., Hong, C.H., Heo, J., Lim, J.I., Yang, H.J.: Controlled mutual quantum entity authentication using entanglement swapping. Chin. Phys. B **24**, 090306 (2015)
52. Gao, G., Wang, Y.: Cryptanalysis of controlled mutual quantum entity authentication using entanglement swapping. Commun. Theor. Phys. **67**(1), 33–36 (2017)
53. Ingemarsson, I., Simmons, G.J.: A protocol to set up shared secret schemes without the assistance of a mutually trusted party. In: Advances in Cryptology—Proceedings of Eurocrypt'90, pp. 266–282. Springer, Berlin (1991)
54. Gao, G., Fang, M., Cheng, M.T.: Cryptanalysis and improvement of a quantum network system of QSS-QDC using chi-type entangled states. Chin. Phys. Lett. **29**, 110305 (2012)
55. Heo, J., Kang, M.S., Hong, C.H., Yang, H., Choi, S.G.: Schemes generating entangled states and entanglement swapping between photons and three-level atoms inside optical cavities for quantum communication. Quantum Inf. Process. **16**, 24 (2017)

56. Heo, J., Kang, M.S., Hong, C.H., Choi, S.G., Hong, J.P.: Constructions of secure entanglement channels assisted by quantum dots inside single-sided optical cavities. Opt. Commun. **396**, 239 (2017)
57. Li, C.Y., Zhou, H.Y., Wang, Y., Deng, F.G.: Secure quantum key distribution network with Bell states and local unitary operations. Chin. Phys. Lett. **22**, 1049 (2005)
58. Li, C.Y., Li, X.H., et al.: Efficient quantum cryptography network without entanglement and quantum memory. Chin. Phys. Lett. **23**, 2896 (2006)
59. Yoon, C.S., Kang, M.S., Lim, J.I., Yang, H.J.: Quantum signature scheme based on a quantum search algorithm. Phys. Scr. **90**, 015103 (2015)
60. Hong, C.H., Lim, J.I., Kim, J.I., Yang, H.J.: Two-way quantum direct communication protocol using entanglement swapping. Korean Phys. Soc. **56**, 1733 (2010)
61. Hong, C.H., Heo, J., Jang, J.G., Kwon, D.: Quantum identity authentication with single photon. Quantum Inf. Process. **16**(10), 236–2181 (2017)