Quantum Information Processing (2020) 19:124
https://doi.org/10.1007/s11128-020-2608-8

Response to "Comment on 'Controlled mutual quantum entity authentication with an untrusted third party'"

Min-Sung Kang[1,2] · Jino Heo[3] · Chang-Ho Hong[4] · Hyung-Jin Yang[5,6] · Sung Moon[1] · Sang-Wook Han[1,7]

Received: 24 January 2019 / Accepted: 5 February 2020 / Published online: 2 March 2020

Abstract
Recently, Wang et al. (Quantum Inf Process, QINP-D-18-00478R1, 2019) commented that a third party can obtain an authentication key from communicating parties by performing an entanglement swapping attack on the controlled mutual quantum entity authentication (CMQEA) protocol. In this response, we apply this attack to the CMQEA protocol and analyze whether this claim is actually valid. From the analysis, we provide a confirmation that this attack can be prevented using existing countermeasures. In addition, we propose an improved protocol that is fundamentally robust to entanglement swapping attack.

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

This is the reply to the commentary https://doi.org/10.1007/s11128-020-2611-0.

✉ 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 Korean Intellectual Property Office, Government Complex Daejeon Building 4, 189, Cheongsa-ro, Seo-gu, Daejeon 35208, Republic of Korea

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

4 National Security Research Institute, P. O. Box 1, Youseng, Daejeon 34188, Republic of Korea

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

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

7 Division of Nano and Information Technology, Korea Institute of Science and Technology School, Korea University of Science and Technology, Seoul 02792, South Korea

1 Introduction

Controlled mutual quantum entity authentication (CMQEA) is a protocol in which communicating parties Alice and Bob confirm each other's identities under the control of a third party, Charlie, in a quantum network composed of Greenberger–Horne–Zeilinger (GHZ)-like states [1, 2]. However, an internal attack by an untrusted Charlie was not considered when the CMQEA protocol was first proposed in 2015 [3]. In 2018, Kang et al. proposed an entanglement-checking method and a random number method to address this security loophole [1]. Recently, Wang et al. proposed that an untrusted Charlie could obtain an authentication key through an entanglement swapping attack on the CMQEA [4]. We have identified errors in this claim. In this study, we modified their claim and re-applied the entanglement swapping attack to the original CMQEA protocol. In addition, we confirmed that an eavesdropper Eve has a probability of $1/2^N$ to obtain the authentication keys in the N GHZ-like state sequences with this attack. Finally, we summarize the countermeasures proposed in previous papers to prevent such attacks. We confirm that these existing countermeasures can prevent this attack and explain the features of these countermeasures. In addition, we propose an improved protocol that is fundamentally robust to entanglement swapping attack.

2 Brief review of controlled mutual quantum entity authentication protocol

Before describing the entanglement swapping attacks presented by Wang et al., we briefly introduce the CMQEA protocol. In the CMQEA protocol [1, 2], through the preparation and security-checking phases, Charlie shares the GHZ-like states

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

with Alice and Bob. The subscripts $(2i-1)$ and $(2i)$ refer to the odd-numbered and even-numbered qubits, respectively, in the qubit sequence. In addition, the subscripts A, B, and C represent the owner of a particular qubit. Then, in the entity authentication phase, Alice and Bob authenticate each other under the control of Charlie as follows:

E1 Charlie randomly selects one communication member, Alice or Bob, to apply the Pauli operation $\sigma_{k_i} \in \{\sigma_{00} = I, \sigma_{01} = \sigma_x, \sigma_{10} = i\sigma_y, \sigma_{11} = \sigma_z\}$, which corresponds to the pre-shared authentication key $k_i \in \{00, 01, 10, 11\}$, for the qubit $(2i-1)A$ or $(2i)B$ in Eq. (1). If Charlie selects Alice, Alice applies the Pauli operator σ_{k_i} to the qubit $(2i-1)A$. If Charlie selects Bob, Bob applies the Pauli operator σ_{k_i} to the qubit $(2i)B$.
E2 Charlie executes the σ_z-basis measurement on the qubits $\{(2i-1)C, (2i)C\}$ in Eq. (1), and his measurement outcomes are $c_{2i-1}c_{2i} \in \{00, 01, 10, 11\}$. After Charlie's measurement, the GHZ-like state of Eq. (1) collapses 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 perform Bell-basis measurements on the qubits, $\{(2i-1)A, (2i)A\}$ and $\{(2i-1)B, (2i)B\}$, respectively; this is called entanglement swapping. 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 $2i$).

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

3 Analysis of Wang et al.'s entanglement swapping attack

Wang et al. claimed that an untrusted third party could obtain an authentication key that was pre-shared by Alice and Bob by performing entanglement swapping in the CMQEA protocol [4]. In their paper, Wang et al. explained that, unlike the **E2** and **E3** phase of Sect. 2, a third party can learn what operator was applied by Alice or Bob if they perform a Bell measurement on the $(2i)C$ and $(2i-1)C$ qubits of GHZ-like states. Here, the operator corresponds to the authentication key. Therefore, if Charlie knows the specific operator $\sigma_{k_i} \in \{\sigma_{00} = I, \sigma_{01} = \sigma_x, \sigma_{10} = i\sigma_y, \sigma_{11} = \sigma_z\}$, he can naturally know what the authentication key $k_i \in \{00, 01, 10, 11\}$ is. For example, in the P2 phase, with an untrusted Charlie and Eve, GHZ-like states

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

of Eq. (2) are prepared in Ref. [4]. Subsequently, Alice applied the operator σ_x, and Charlie attempted the entanglement swapping attack as in Eq. (6) of Ref [3] as follows:

$$\begin{aligned}\sigma_x|\xi\rangle_{(2i-1)ABC} \otimes |\xi\rangle_{(2i)ABC} = \frac{1}{2\sqrt{2}}\Big(&|\Psi^+\rangle_{(2i-1)(2i)A}|\Phi^+\rangle_{(2i-1)(2i)B}|\Phi^+\rangle_{(2i-1)(2i)C} \\ &+ |\Phi^+\rangle_{(2i-1)(2i)A}|\Psi^+\rangle_{(2i-1)(2i)B}|\Phi^+\rangle_{(2i-1)(2i)C} \\ &- |\Psi^-\rangle_{(2i-1)(2i)A}|\Phi^-\rangle_{(2i-1)(2i)B}|\Phi^-\rangle_{(2i-1)(2i)C} \\ &+ |\Phi^-\rangle_{(2i-1)(2i)A}|\Psi^-\rangle_{(2i-1)(2i)B}|\Phi^-\rangle_{(2i-1)(2i)C} \\ &- |\Phi^+\rangle_{(2i-1)(2i)A}|\Phi^+\rangle_{(2i-1)(2i)B}|\Psi^+\rangle_{(2i-1)(2i)C} \\ &+ |\Psi^+\rangle_{(2i-1)(2i)A}|\Psi^+\rangle_{(2i-1)(2i)B}|\Psi^+\rangle_{(2i-1)(2i)C} \\ &- |\Phi^-\rangle_{(2i-1)(2i)A}|\Phi^-\rangle_{(2i-1)(2i)B}|\Psi^-\rangle_{(2i-1)(2i)C} \\ &+ |\Psi^-\rangle_{(2i-1)(2i)A}|\Psi^-\rangle_{(2i-1)(2i)B}|\Psi^-\rangle_{(2i-1)(2i)C}\Big)\end{aligned} \tag{3}$$

If the Bell measurement results of Alice, Bob, and Charlie are $\left|\Psi^{+}\right\rangle_{(2i-1)(2i)A}$, $\left|\Phi^{+}\right\rangle_{(2i-1)(2i)B}$, and $\left|\Phi^{+}\right\rangle_{(2i-1)(2i)C}$, respectively, the operation of Alice must be σ_x. Consequently, Charlie can guess that the authentication key $k_i = 01$.

As described above, according to Wang et al.'s argument, an untrusted Charlie can obtain Alice and Bob's authentication keys perfectly by performing an entanglement swapping attack on the CMQEA protocol. However, there is a fallacy in their argument. The GHZ state of Eq. (2) that they use to describe the attack differs from the GHZ state of Eq. (1) used by the original protocol. This difference causes the protocol to ultimately fail, resulting in Charlie's misconduct. In the original CMQEA protocol, as can be seen in Table 4 of Ref. [2], even though Alice's measurement outcome is 10, Bob's measurement outcomes are randomly generated as 00, 01, 10, and 11. Therefore, because the original protocol uses N GHZ-like state sequences for authentication, Bob's measurement outcomes must be uniformly distributed. However, in the example of Wang et al., such as in Eq. (3), if Alice's measurement outcome $a_{2i-1}a_{2i}$ is $\left|\Psi^{+}\right\rangle_{(2i-1)(2i)A}$: 10, Bob's measurement outcome $b_{2i-1}b_{2i}$ is always $\left|\Phi^{+}\right\rangle_{(2i-1)(2i)B}$: 00 or $\left|\Psi^{+}\right\rangle_{(2i-1)(2i)B}$: 10. In such a situation, when using N GHZ-like state sequences, Bob's measurement outcomes are not uniformly distributed, and Charlie's attack eventually becomes apparent. Therefore, we should verify the validity of Charlie's attempts at an entanglement swapping attack on the GHZ-like states of Eq. (1). The GHZ-like states of Eq. (1) are rearranged as follows:

$$\begin{aligned}|\xi\rangle_{(2i-1)ABC}\otimes|\xi\rangle_{(2i)ABC} = \frac{1}{2}\Big(&\left|\Psi^{+}\right\rangle_{(2i-1)AB}\left|\Phi^{-}\right\rangle_{(2i)AB}|0\rangle_{(2i-1)C}|0\rangle_{(2i)C}\\ &-\left|\Psi^{+}\right\rangle_{(2i-1)AB}\left|\Psi^{+}\right\rangle_{(2i)AB}|0\rangle_{(2i-1)C}|1\rangle_{(2i)C}\\ &+\left|\Phi^{+}\right\rangle_{(2i-1)AB}\left|\Phi^{-}\right\rangle_{(2i)AB}|1\rangle_{(2i-1)C}|0\rangle_{(2i)C}\\ &+\left|\Phi^{+}\right\rangle_{(2i-1)AB}\left|\Psi^{+}\right\rangle_{(2i)AB}|0\rangle_{(2i-1)C}|1\rangle_{(2i)C}\Big)\end{aligned} \tag{4}$$

In the **E1** phase of Sect. 2, if Charlie selects Alice and then Alice applies Pauli operators $\sigma_{k_i} \in \left\{\sigma_{00} = I, \sigma_{01} = \sigma_x, \sigma_{10} = i\sigma_y, \sigma_{11} = \sigma_z\right\}$ to the qubits $(2i-1)A$ of GHZ-like states in Eq. (4), these states become

$$\begin{aligned}&|\xi\rangle_{(2i-1)ABC}\otimes|\xi\rangle_{(2i)ABC}\\ &= \frac{1}{2}\Big[\left(|\mathrm{Rev}+-\rangle_{(2i-1)(2i)AB}+|\mathrm{Rev}++\rangle_{(2i-1)(2i)AB}\right)\left|\Phi^{+}\right\rangle_{(2i-1)(2i)C}\\ &\quad+\left(|\mathrm{Rev}+-\rangle_{(2i-1)(2i)AB}-|\mathrm{Rev}++\rangle_{(2i-1)(2i)AB}\right)\left|\Phi^{-}\right\rangle_{(2i-1)(2i)C}\\ &\quad-\left(|\mathrm{ID}++\rangle_{(2i-1)(2i)AB}-|\mathrm{ID}+-\rangle_{(2i-1)(2i)AB}\right)\left|\Psi^{+}\right\rangle_{(2i-1)(2i)C}\\ &\quad-\left(|\mathrm{ID}++\rangle_{(2i-1)(2i)AB}+|\mathrm{ID}+-\rangle_{(2i-1)(2i)AB}\right)\left|\Psi^{-}\right\rangle_{(2i-1)(2i)C}\Big],\end{aligned} \tag{5}$$

$$\begin{aligned}&\sigma_x|\xi\rangle_{(2i-1)ABC}\otimes|\xi\rangle_{(2i)ABC}\\ &= \frac{1}{2}\Big[\left(|\mathrm{ID}+-\rangle_{(2i-1)(2i)AB}+|\mathrm{ID}++\rangle_{(2i-1)(2i)AB}\right)\left|\Phi^{+}\right\rangle_{(2i-1)(2i)C}\\ &\quad+\left(|\mathrm{ID}+-\rangle_{(2i-1)(2i)AB}-|\mathrm{ID}++\rangle_{(2i-1)(2i)AB}\right)\left|\Phi^{-}\right\rangle_{(2i-1)(2i)C}\end{aligned}$$

$$
\begin{aligned}
&- \left(|\mathrm{Rev}++\rangle_{(2i-1)(2i)AB} - |\mathrm{Rev}+-\rangle_{(2i-1)(2i)AB}\right)\left|\Psi^{+}\right\rangle_{(2i-1)(2i)C} \\
&- \left(|\mathrm{Rev}++\rangle_{(2i-1)(2i)AB} + |\mathrm{Rev}+-\rangle_{(2i-1)(2i)AB}\right)\left|\Psi^{-}\right\rangle_{(2i-1)(2i)C}\Big], \qquad (6)
\end{aligned}
$$

$$
\begin{aligned}
&i\sigma_y|\xi\rangle_{(2i-1)ABC}\otimes|\xi\rangle_{(2i)ABC} \\
&= \frac{1}{2}\Big[\left(|\mathrm{ID}++\rangle_{(2i-1)(2i)AB} + |\mathrm{ID}+-\rangle_{(2i-1)(2i)AB}\right)\left|\Phi^{+}\right\rangle_{(2i-1)(2i)C} \\
&+ \left(|\mathrm{ID}++\rangle_{(2i-1)(2i)AB} - |\mathrm{ID}+-\rangle_{(2i-1)(2i)AB}\right)\left|\Phi^{-}\right\rangle_{(2i-1)(2i)C} \\
&- \left(|\mathrm{Rev}+-\rangle_{(2i-1)(2i)AB} - |\mathrm{Rev}++\rangle_{(2i-1)(2i)AB}\right)\left|\Psi^{+}\right\rangle_{(2i-1)(2i)C}, \\
&- \left(|\mathrm{Rev}+-\rangle_{(2i-1)(2i)AB} + |\mathrm{Rev}++\rangle_{(2i-1)(2i)AB}\right)\left|\Psi^{-}\right\rangle_{(2i-1)(2i)C}\Big], \qquad (7)
\end{aligned}
$$

and

$$
\begin{aligned}
&\sigma_z|\xi\rangle_{(2i-1)ABC}\otimes|\xi\rangle_{(2i)ABC} \\
&= \frac{1}{2}\Big[\left(|\mathrm{Rev}++\rangle_{(2i-1)(2i)AB} + |\mathrm{Rev}+-\rangle_{(2i-1)(2i)AB}\right)\left|\Phi^{+}\right\rangle_{(2i-1)(2i)C} \\
&+ \left(|\mathrm{Rev}++\rangle_{(2i-1)(2i)AB} - |\mathrm{Rev}+-\rangle_{(2i-1)(2i)AB}\right)\left|\Phi^{-}\right\rangle_{(2i-1)(2i)C} \\
&- \left(|\mathrm{ID}+-\rangle_{(2i-1)(2i)AB} - |\mathrm{ID}++\rangle_{(2i-1)(2i)AB}\right)\left|\Psi^{+}\right\rangle_{(2i-1)(2i)C} \\
&- \left(|\mathrm{ID}+-\rangle_{(2i-1)(2i)AB} + |\mathrm{ID}++\rangle_{(2i-1)(2i)AB}\right)\left|\Psi^{-}\right\rangle_{(2i-1)(2i)C}\Big] \qquad (8)
\end{aligned}
$$

respectively. Here, $|\mathrm{Rev}+-\rangle_{(2i-1)(2i)AB} = \left|\Psi^{+}\right\rangle_{(2i-1)AB}\left|\Phi^{-}\right\rangle_{(2i)AB}$, $|\mathrm{ID}++\rangle_{(2i-1)(2i)AB} = \left|\Psi^{+}\right\rangle_{(2i-1)AB}\left|\Psi^{+}\right\rangle_{(2i)AB}$, $|\mathrm{ID}+-\rangle_{(2i-1)(2i)AB} = \left|\Phi^{+}\right\rangle_{(2i-1)AB}\left|\Phi^{-}\right\rangle_{(2i)AB}$, and $|\mathrm{Rev}++\rangle_{(2i-1)(2i)AB} = \left|\Phi^{+}\right\rangle_{(2i-1)AB}\left|\Psi^{+}\right\rangle_{(2i)AB}$. Note that Bell states $\left|\Phi^{+}\right\rangle$, $\left|\Phi^{-}\right\rangle$, $\left|\Psi^{+}\right\rangle$, and $\left|\Psi^{-}\right\rangle$ are representative of two entangled states and are unitarily transformed by local operations, as shown in Fig. 1. Therefore, the symbols ID + +, ID + −, Rev + +, and Rev + − indicate the relationship between the two states. For example, in Fig. 1, applying a local operator $I\otimes\sigma_x$ or $\sigma_x\otimes I$ to $\left|\Phi^{+}\right\rangle$ results in $\left|\Psi^{+}\right\rangle$:

$$
\left|\boldsymbol{\Phi}^{+}\right\rangle \rightarrow \left|\boldsymbol{\Psi}^{+}\right\rangle = (\boldsymbol{I}\otimes\boldsymbol{\sigma_x})\left|\boldsymbol{\Phi}^{+}\right\rangle = (\boldsymbol{I}\otimes\boldsymbol{\sigma_x})\frac{\mathbf{1}}{\sqrt{\mathbf{2}}}(|\mathbf{00}\rangle + |\mathbf{11}\rangle) = \frac{\mathbf{1}}{\sqrt{\mathbf{2}}}(|\mathbf{01}\rangle + |\mathbf{10}\rangle) \qquad (9)
$$

$$
\left|\boldsymbol{\Phi}^{+}\right\rangle \rightarrow \left|\boldsymbol{\Psi}^{+}\right\rangle = (\boldsymbol{\sigma_x}\otimes\boldsymbol{I})\left|\boldsymbol{\Phi}^{+}\right\rangle = (\boldsymbol{\sigma_x}\otimes\boldsymbol{I})\frac{\mathbf{1}}{\sqrt{\mathbf{2}}}(|\mathbf{00}\rangle + |\mathbf{11}\rangle) = \frac{\mathbf{1}}{\sqrt{\mathbf{2}}}(|\mathbf{01}\rangle + |\mathbf{10}\rangle) \qquad (10)
$$

We define Rev + + as the relationship between $\left|\Phi^{+}\right\rangle$ and $\left|\Psi^{+}\right\rangle$ where the bit flips σ_x. Additionally, applying a local operator $I\otimes\sigma_z$ or $\sigma_z\otimes I$ to $\left|\Phi^{+}\right\rangle$ results in $\left|\Phi^{-}\right\rangle$:

$$
\left|\boldsymbol{\Phi}^{+}\right\rangle \rightarrow \left|\boldsymbol{\Phi}^{-}\right\rangle = (\boldsymbol{I}\otimes\boldsymbol{\sigma_z})\left|\boldsymbol{\Phi}^{+}\right\rangle = (\boldsymbol{I}\otimes\boldsymbol{\sigma_z})\frac{\mathbf{1}}{\sqrt{\mathbf{2}}}(|\mathbf{00}\rangle + |\mathbf{11}\rangle) = \frac{\mathbf{1}}{\sqrt{\mathbf{2}}}(|\mathbf{00}\rangle - |\mathbf{11}\rangle) \qquad (11)
$$

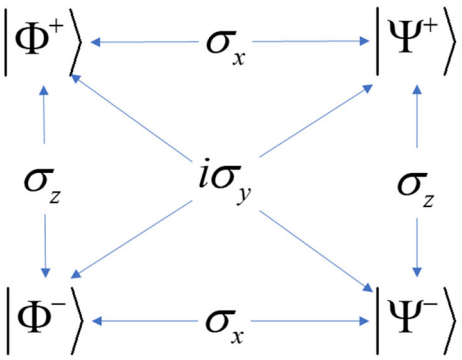

Fig. 1 Unitary transformation of Bell states by local operations

$$|\boldsymbol{\Phi}^+\rangle \rightarrow |\boldsymbol{\Phi}^-\rangle = (\boldsymbol{\sigma}_z \otimes \boldsymbol{I})|\boldsymbol{\Phi}^+\rangle = (\boldsymbol{\sigma}_z \otimes \boldsymbol{I})\frac{\mathbf{1}}{\sqrt{\mathbf{2}}}(|\mathbf{00}\rangle + |\mathbf{11}\rangle) = \frac{\mathbf{1}}{\sqrt{\mathbf{2}}}(|\mathbf{00}\rangle - |\mathbf{11}\rangle) \tag{12}$$

We define ID + − as the relationship between $|\Phi^+\rangle$ and $|\Phi^-\rangle$ where the phase flips σ_z. Furthermore, applying a local operator $I \otimes i\sigma_y$ or $i\sigma_y \otimes I$ to $|\Phi^+\rangle$ results in $|\Psi^-\rangle$:

$$|\boldsymbol{\Phi}^+\rangle \rightarrow |\boldsymbol{\Psi}^-\rangle = (\boldsymbol{I} \otimes \boldsymbol{\sigma}_z)|\boldsymbol{\Phi}^+\rangle = (\boldsymbol{I} \otimes \boldsymbol{\sigma}_z)\frac{\mathbf{1}}{\sqrt{\mathbf{2}}}(|\mathbf{00}\rangle + |\mathbf{11}\rangle) = \frac{\mathbf{1}}{\sqrt{\mathbf{2}}}(|\mathbf{00}\rangle - |\mathbf{11}\rangle) \tag{13}$$

$$|\boldsymbol{\Phi}^+\rangle \rightarrow |\boldsymbol{\Psi}^-\rangle = (\boldsymbol{\sigma}_z \otimes \boldsymbol{I})|\boldsymbol{\Phi}^+\rangle = (\boldsymbol{\sigma}_z \otimes \boldsymbol{I})\frac{\mathbf{1}}{\sqrt{\mathbf{2}}}(|\mathbf{00}\rangle + |\mathbf{11}\rangle) = \frac{\mathbf{1}}{\sqrt{\mathbf{2}}}(|\mathbf{00}\rangle - |\mathbf{11}\rangle) \tag{14}$$

We define Rev + − as the relationship between $|\Phi^+\rangle$ and $|\Psi^-\rangle$ where the bit and phase flips $i\sigma_y$. Finally, if $|\Phi^+\rangle$ and $|\Phi^+\rangle$ are identical, we define ID++. These principles have been applied to $|\mathrm{ID}++\rangle$, $|\mathrm{ID}+-\rangle$, $|\mathrm{Rev}++\rangle$, and $|\mathrm{Rev}+-\rangle$, and the details of these are as follows.

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

$$\begin{aligned}|\mathrm{ID}++\rangle &= |\Psi^+\rangle_{(2i-1)AB}|\Psi^+\rangle_{(2i)AB} \\ &= \frac{1}{2}\Big(|\Phi^+\rangle_{(2i-1)(2i)A}|\Phi^+\rangle_{(2i-1)(2i)B} - |\Phi^-\rangle_{(2i-1)(2i)A}|\Phi^-\rangle_{(2i-1)(2i)B} \\ &\quad + |\Psi^+\rangle_{(2i-1)(2i)A}|\Psi^+\rangle_{(2i-1)(2i)B} - |\Psi^-\rangle_{(2i-1)(2i)A}|\Psi^-\rangle_{(2i-1)(2i)B}\Big),\end{aligned} \tag{16}$$

$$|\mathrm{ID}+-\rangle = |\Phi^+\rangle_{(2i-1)AB}|\Phi^-\rangle_{(2i)AB}$$

$$= \frac{1}{2}\Big(\left|\Phi^{+}\right\rangle_{(2i-1)(2i)A}\left|\Phi^{-}\right\rangle_{(2i-1)(2i)B} + \left|\Phi^{-}\right\rangle_{(2i-1)(2i)A}\left|\Phi^{+}\right\rangle_{(2i-1)(2i)B} - \left|\Psi^{+}\right\rangle_{(2i-1)(2i)A}\left|\Psi^{-}\right\rangle_{(2i-1)(2i)B} - \left|\Psi^{-}\right\rangle_{(2i-1)(2i)A}\left|\Psi^{+}\right\rangle_{(2i-1)(2i)B}\Big), \tag{17}$$

and

$$\begin{aligned}|\mathrm{Rev}++\rangle &= \left|\Phi^{+}\right\rangle_{(2i-1)AB}\left|\Psi^{+}\right\rangle_{(2i)AB} \\ &= \frac{1}{2}\Big(\left|\Phi^{+}\right\rangle_{(2i-1)(2i)A}\left|\Psi^{+}\right\rangle_{(2i-1)(2i)B} + \left|\Phi^{-}\right\rangle_{(2i-1)(2i)A}\left|\Psi^{-}\right\rangle_{(2i-1)(2i)B} \\ &\quad + \left|\Psi^{+}\right\rangle_{(2i-1)(2i)A}\left|\Phi^{+}\right\rangle_{(2i-1)(2i)B} + \left|\Psi^{-}\right\rangle_{(2i-1)(2i)A}\left|\Phi^{-}\right\rangle_{(2i-1)(2i)B}\Big).\end{aligned} \tag{18}$$

As can be seen from Eqs. (5) and (8), $|\xi\rangle_{(2i-1)ABC} \otimes |\xi\rangle_{(2i)ABC}$ of Eq. (5) and σ_z $|\xi\rangle_{(2i-1)ABC} \otimes |\xi\rangle_{(2i)ABC}$ of Eq. (8) are identical except for the sign $\pm$ of the relative phase. Therefore, Charlie cannot accurately estimate the operator I or σ_z applied by Alice with Bell measurement outcomes of Alice and Bob for the GHZ-like state of Eqs. (5) and (8). For example, suppose that the Bell measurement outcomes of Alice and Bob are $|\mathrm{Rev}+-\rangle_{(2i-1)(2i)AB}$ and the measurement outcomes of Charlie are $\left|\Phi^{+}\right\rangle_{(2i-1)(2i)C}$. Because these measurements can occur in both $|\xi\rangle_{(2i-1)ABC} \otimes |\xi\rangle_{(2i)ABC}$ of Eq. (5) and $\sigma_z|\xi\rangle_{(2i-1)ABC} \otimes |\xi\rangle_{(2i)ABC}$ of Eq. (8), Charlie cannot determine whether Alice used the I or σ_z operators. Similarly, as can be seen from Eqs. (6) and (7), $\sigma_x|\xi\rangle_{(2i-1)ABC} \otimes |\xi\rangle_{(2i)ABC}$ of Eq. (6) and $i\sigma_y|\xi\rangle_{(2i-1)ABC} \otimes |\xi\rangle_{(2i)ABC}$ of Eq. (7) are identical except for the sign $\pm$ of relative phase. Therefore, Charlie cannot accurately guess the operator σ_x or $\mathrm{i}\sigma_y$ applied by Alice with the Bell measurement outcomes of Alice and Bob for the GHZ-like state of Eqs. (6) and (7). As another example, suppose that the Bell measurement outcomes of Alice and Bob are $|\mathrm{ID}+-\rangle_{(2i-1)(2i)AB}$ and the measurement outcomes of Charlie are $\left|\Phi^{-}\right\rangle_{(2i-1)(2i)C}$. Because these measurements can occur in both $\sigma_x|\xi\rangle_{(2i-1)ABC} \otimes |\xi\rangle_{(2i)ABC}$ of Eq. (6) and $i\sigma_y|\xi\rangle_{(2i-1)ABC} \otimes |\xi\rangle_{(2i)ABC}$ of Eq. (7), Charlie cannot determine whether Alice used the σ_x or $\mathrm{i}\sigma_y$ operators. Consequently, Charlie can only estimate one of the two bits of the authentication key $k_i \in \{00, 01, 10, 11\}$. Therefore, because the CMQEA protocol [1, 2] uses N GHZ-like state sequences $\otimes_{i=1}^{N}|\xi\rangle_{(2i-1)ABC}|\xi\rangle_{(2i)ABC}$, the probability that Charlie obtains an authentication key sequence $K = (k_1, k_2, k_3, \ldots, k_N)$ through an entanglement swapping attack is $1/2^N$.

In addition to the probabilistic analysis thus far, the analysis in terms of information theory is as follows. If I_{E} is the amount of information Eve can obtain from Alice and Bob's measurement outcomes, then I_E can be described as $I_{\mathrm{E}} = H(k_i) - H(k_i|a_{2i-1}a_{2i}, b_{2i-1}b_{2i})$ [5]. Here, $H(X)$ is the Shannon entropy of the random variable X. $H(k_i) = 2$ because the key $k_i \in \{00, 01, 10, 11\}$ is two bits of information. And, if $(a_{2i-1}a_{2i}, b_{2i-1}b_{2i}) = |\mathrm{Rev}+\pm\rangle$, $k_i \in \{00, 11\}$; if $(a_{2i-1}a_{2i}, b_{2i-1}b_{2i}) = |\mathrm{ID}+\pm\rangle$, $k_i \in \{01, 10\}$. Therefore, $H(k_i|a_{2i-1}a_{2i}, b_{2i-1}b_{2i}) = 1$. As a result, $I_{\mathrm{E}} = 1$, which means that 1 bit out of 2 bits is leaked.

4 Countermeasures against entanglement swapping attack

In this section, we explain three countermeasures to prevent an entanglement swapping attack: GHZ-like state sequences method, random number method, and honesty-checking method. Here, GHZ-like state sequence and random number methods were proposed to prevent outsider attacks in the original CMQEA protocol [2, 3] in 2015 and insider attacks by Gao in the improved CMQEA protocol [1] in 2018, respectively. In this section, we confirm in that both methods can prevent the entanglement swapping attack. The honesty-checking method has already been proposed by Wang as a countermeasure against the entanglement swapping attack.

As described in Sect. 2, the probability of an untrusted Charlie guessing an authentication key sequence through an entanglement swapping attack on the CMQEA protocol using N GHZ-like state sequences is $1/2^N$. The first countermeasure is to increase the number of N states used in the protocol so that the entanglement swapping attack probability is very small. For example, if N is 7, the probability of a successful attack is 0.78%. This means that an entanglement swapping attack is virtually impossible. However, this method is a passive countermeasure in which the 2-bit authentication key used for each session is guessed to have a 50% probability.

The second countermeasure was proposed by Wang et al. in a comment paper [4], and it is an honesty-checking method. In this method, Alice and Bob actively verify Charlie's honesty by randomly selecting from the sequence of GHZ-like states before the **E3** phase of Sect. 2. Here, the honesty-checking method is the same as the entanglement correlation check method and is well described in Ref [1]. For example, suppose Alice and Bob select $(2j-1)$th and $(2j)$th GHZ-like states $|\boldsymbol{\xi}\rangle_{(\boldsymbol{2j-1})\boldsymbol{ABC}}$ and $|\boldsymbol{\xi}\rangle_{(\boldsymbol{2j})\boldsymbol{ABC}}$:

$$\begin{aligned}|\boldsymbol{\xi}\rangle_{(\boldsymbol{2j-1})\boldsymbol{ABC}} &= \frac{\mathbf{1}}{\sqrt{\mathbf{2}}}\left(\left|\boldsymbol{\Psi}^{+}\right\rangle_{(\boldsymbol{2j-1})\boldsymbol{AB}}|\mathbf{0}\rangle_{(\boldsymbol{2j-1})\boldsymbol{C}} + \left|\boldsymbol{\Phi}^{+}\right\rangle_{(\boldsymbol{2j-1})\boldsymbol{AB}}|\mathbf{1}\rangle_{(\boldsymbol{2j-1})\boldsymbol{C}}\right)\\ &= \frac{\mathbf{1}}{\sqrt{\mathbf{2}}}(|\boldsymbol{x}+\rangle|\boldsymbol{x}+\rangle|\boldsymbol{x}+\rangle - |\boldsymbol{x}-\rangle|\boldsymbol{x}-\rangle|\boldsymbol{x}-\rangle)_{(\boldsymbol{2j-1})\boldsymbol{ABC}} \end{aligned} \tag{19}$$

$$\begin{aligned}|\boldsymbol{\xi}\rangle_{(\boldsymbol{2j})\boldsymbol{ABC}} &= \frac{\mathbf{1}}{\sqrt{\mathbf{2}}}\left(\left|\boldsymbol{\Phi}^{-}\right\rangle_{(\boldsymbol{2j})\boldsymbol{AB}}|\mathbf{0}\rangle_{(\boldsymbol{2j})\boldsymbol{C}} - \left|\boldsymbol{\Psi}^{+}\right\rangle_{(\boldsymbol{2j})\boldsymbol{AB}}|\mathbf{1}\rangle_{(\boldsymbol{2j})\boldsymbol{C}}\right)\\ &= \frac{\mathbf{1}}{\sqrt{\mathbf{2}}}(|\boldsymbol{y}+\rangle|\boldsymbol{y}+\rangle|\boldsymbol{y}+\rangle - |\boldsymbol{y}-\rangle|\boldsymbol{y}-\rangle|\boldsymbol{y}-\rangle)_{(\boldsymbol{2j})\boldsymbol{ABC}} \end{aligned} \tag{20}$$

Here, $|x+\rangle$ and $|\boldsymbol{x}-\rangle$ are the eigenstates of σ_x, and $|y+\rangle$ and $|y-\rangle$ are the eigenstates of σ_y. Then, Alice and Bob inform Charlie of the location of the $(2j-1)$th state and the measurement base σ_z or σ_x. They also inform Charlie of the location of the $(2j)$th state and the measurement base σ_z or σ_y. Charlie measures the $(2j-1)$th state of Eq. (19) with the base σ_z or σ_x and the $(2j)$th state of Eq. (20) with the base σ_z or σ_y and announces each outcome with the basis to Alice and Bob. Alice and Bob then measure each $(2j-1)$th and $(2j)$th state on the same basis as Charlie. The outcomes of these measurements should be in accordance with Tables 1 and 2; otherwise, Charlie is deemed to have committed fraud. Because Alice and Bob perform this method before performing the Bell measurement of E3 phase in Sect. 2, this method can block

Table 1 Measurement outcomes from the honesty-check of the $(2j-1)$th state in Eq. (19)

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	$x+:\|x+\rangle_{(2j-1)C}$	$x+:\|x+\rangle_{(2j-1)A}$	$x+:\|x+\rangle_{(2j-1)B}$
	$x-:\|x-\rangle_{(2j-1)C}$	$x-:\|x-\rangle_{(2j-1)A}$	$x-:\|x-\rangle_{(2j-1)B}$

Table 2 Measurement outcomes from the honesty-check of the $(2j)$th state in Eq. (20)

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

Charlie's malicious behavior and is an active countermeasure. Hence, Alice and Bob's authentication keys are not exposed. The only disadvantage of this method is that it requires some state consumption for honesty-checking.

As a final countermeasure, Alice and Bob can use a random number to defend themselves against Eve's attack. This method has already been proposed to prevent Charlie's internal attack in the CMQEA protocol [1], and Alice and Bob use it after encrypting the authentication key with each random number. The proposed method involves using a random number; the protocol that modifies the entity authentication phase is described below [1].

E1′ (a) Alice and Bob prepare random numbers $r_{(i)A}$ and $r_{(i)B}$, where $r_{(i)A}, r_{(i)B} \in \{00, 01, 10, 11\}$. Then, they encrypt their previously shared authentication key k_i with their own random numbers $r_{(i)A}$ and $r_{(i)B}$:

$$\boldsymbol{k_{(i)A} = k_i \oplus r_{(i)A}} \tag{21}$$

$$\boldsymbol{k_{(i)B} = k_i \oplus r_{(i)B}} \tag{22}$$

Here, symbol $\oplus$ indicates exclusive or, XOR.

E1′ (b) Charlie randomly selects only one from among Alice or Bob. If Charlie selects Alice, Alice applies the Pauli operator $\sigma_{\boldsymbol{k}_{(i)A}}$ corresponding to the encrypted authentication key $\boldsymbol{k}_{(i)A} = \boldsymbol{k}_i \oplus r_{(i)A}$ of Eq. (21) to the qubit $A_{(2i-1)}$:

$$\begin{aligned}
&\sigma_{\boldsymbol{k}_{(i)A}}|\xi\rangle_{(2i-1)ABC} \otimes |\xi\rangle_{(2i)ABC} \\
&= \frac{1}{\sqrt{2}}\Big[\big(\sigma_{\boldsymbol{k}_{(i)A}} \otimes \boldsymbol{I}\big)\big|\Psi^+\big\rangle_{(2i-1)AB}|\boldsymbol{0}\rangle_{(2i-1)C} + \big(\sigma_{\boldsymbol{k}_{(i)A}} \otimes \boldsymbol{I}\big)\big|\Phi^+\big\rangle_{(2i-1)AB}|\boldsymbol{1}\rangle_{(2i-1)C}\Big] \\
&\quad \otimes \frac{1}{\sqrt{2}}\Big(\big|\Phi^-\big\rangle_{(2i)AB}|\boldsymbol{0}\rangle_{(2i)C} - \big|\Psi^+\big\rangle_{(2i)AB}|\boldsymbol{1}\rangle_{(2i)C}\Big)
\end{aligned} \tag{23}$$

If Charlie selects Bob, Bob applies the Pauli operator corresponding to the classical bit $\boldsymbol{k}_{(i)B} = \boldsymbol{k}_i \oplus r_{(i)B}$ of Eq. (22) to the qubit $B_{(2i)}$:

$$\begin{aligned}
&|\xi\rangle_{(2i-1)ABC} \otimes \sigma_{\boldsymbol{k}_{(i)B}}|\xi\rangle_{(2i)ABC} \\
&= \frac{1}{\sqrt{2}}\Big(\big|\Psi^+\big\rangle_{(2i-1)AB}|\boldsymbol{0}\rangle_{(2i-1)C} + \big|\Phi^+\big\rangle_{(2i-1)AB}|\boldsymbol{1}\rangle_{(2i-1)C}\Big) \\
&\quad \otimes \frac{1}{\sqrt{2}}\Big[\big(\boldsymbol{I} \otimes \sigma_{\boldsymbol{k}_{(i)B}}\big)\big|\Phi^-\big\rangle_{(2i)AB}|\boldsymbol{0}\rangle_{(2i)C} - \big(\boldsymbol{I} \otimes \sigma_{\boldsymbol{k}_{(i)B}}\big)\big|\Psi^+\big\rangle_{(2i)AB}|\boldsymbol{1}\rangle_{(2i)C}\Big]
\end{aligned} \tag{24}$$

Here, $\boldsymbol{k}_i\big(= \boldsymbol{k}_{(i)A} \oplus r_{(i)A} = \boldsymbol{k}_{(i)B} \oplus r_{(i)B}\big)$ is a authentication key pre-shared by Alice and Bob in the preparation phase, $\boldsymbol{k}_i \in \{00, 01, 10, 11\}$.

E2′ Charlie executes the σ_z-basis measurement on the qubits $\big\{C_{(2i-1)}, C_{(2i)}\big\}$ in Eq. (23) or Eq. (24). 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. (23) collapse into

$$\begin{aligned}
c_{2i-1}c_{2i} = 00 &: \Big[\sigma_{k_{(i)A}}\big|\Psi^+\big\rangle_{(2i-1)AB}\Big]\big|\Phi^-\big\rangle_{(2i)AB}, \\
c_{2i-1}c_{2i} = 01 &: \Big[\sigma_{\boldsymbol{k}_{(i)A}}\big|\boldsymbol{\Psi}^+\big\rangle_{\boldsymbol{(2i-1)AB}}\Big]\big|\boldsymbol{\Psi}^+\big\rangle_{\boldsymbol{(2i)AB}}, \\
c_{2i-1}c_{2i} = 10 &: \Big[\sigma_{k_{(i)A}}\big|\Phi^+\big\rangle_{(2i-1)AB}\Big]\big|\Phi^-\big\rangle_{(2i)AB}, \\
\text{or } c_{2i-1}c_{2i} = 11 &: \Big[\sigma_{k_{(i)A}}\big|\Phi^+\big\rangle_{(2i-1)AB}\Big]\big|\boldsymbol{\Psi}^+\big\rangle_{\boldsymbol{(2i)AB}}
\end{aligned} \tag{25}$$

and the GHZ-like states of Eq. (24) collapse into

$$\begin{aligned}
c_{2i-1}c_{2i} = 00 &: \big|\Psi^+\big\rangle_{(2i-1)AB}\Big[\sigma_{k_{(i)B}}\big|\Phi^-\big\rangle_{(2i)AB}\Big], \\
c_{2i-1}c_{2i} = 01 &: \big|\boldsymbol{\Psi}^+\big\rangle_{\boldsymbol{(2i-1)AB}}\big|\Psi^+\big\rangle_{(2i-1)AB}\Big[\sigma_{k_{(i)B}}\big|\boldsymbol{\Psi}^+\big\rangle_{\boldsymbol{(2i)AB}}\Big], \\
c_{2i-1}c_{2i} = 10 &: \big|\Phi^+\big\rangle_{(2i-1)AB}\Big[\sigma_{k_{(i)B}}\big|\Phi^-\big\rangle_{(2i)AB}\Big], \\
\text{or } c_{2i-1}c_{2i} = 11 &: \big|\Phi^+\big\rangle_{(2i-1)AB}\Big[\sigma_{k_{(i)B}}\big|\boldsymbol{\Psi}^+\big\rangle_{\boldsymbol{(2i)AB}}\Big]
\end{aligned} \tag{26}$$

with a 25% probability, and Alice and Bob share one of the pairs of the entangled states. For the first example, when $\boldsymbol{k_i} = 11$ and $r_{(i)A} = 01$, Alice applies the Pauli operator $i\sigma_y\left(= \sigma_{\boldsymbol{k_i}\oplus r_{(i)A}} = \sigma_{10}\right)$ to the qubit $A_{(2i-1)}$ in GHZ-like state of Eq. (25):

$$\begin{aligned}
c_{2i-1}c_{2i} = 00 &: \left[i\sigma_{\mathbf{y}}\left|\Psi^{+}\right\rangle_{(2i-1)AB}\right]\left|\Phi^{-}\right\rangle_{(2i)AB} = \left|\Phi^{-}\right\rangle_{(2i-1)AB}\left|\Phi^{-}\right\rangle_{(2i)AB} = |\mathrm{ID}++\rangle_{(2i-1)(2i)AB},\\
c_{2i-1}c_{2i} = 01 &: \left[i\sigma_{\mathbf{y}}\left|\boldsymbol{\Psi^{+}}\right\rangle_{\boldsymbol{(2i-1)AB}}\right]\left|\boldsymbol{\Psi^{+}}\right\rangle_{\boldsymbol{(2i)AB}} = \left|\Phi^{-}\right\rangle_{(2i-1)AB}\left|\boldsymbol{\Psi^{+}}\right\rangle_{\boldsymbol{(2i)AB}} = |\mathrm{Rev}+-\rangle_{(2i-1)(2i)AB},\\
c_{2i-1}c_{2i} = 10 &: \left[i\sigma_{\mathbf{y}}\left|\Phi^{+}\right\rangle_{(2i-1)AB}\right]\left|\Phi^{-}\right\rangle_{(2i)AB} = \left|\Psi^{-}\right\rangle_{(2i-1)AB}\left|\Phi^{-}\right\rangle_{(2i)AB} = |\mathrm{Rev}++\rangle_{(2i-1)(2i)AB},\\
\text{or } c_{2i-1}c_{2i} = 11 &: \left[i\sigma_{\mathbf{y}}\left|\Phi^{+}\right\rangle_{(2i-1)AB}\right]\left|\boldsymbol{\Psi^{+}}\right\rangle_{\boldsymbol{(2i)AB}} = \left|\Psi^{-}\right\rangle_{(2i-1)AB}\left|\boldsymbol{\Psi^{+}}\right\rangle_{\boldsymbol{(2i)AB}} = |\mathrm{ID}+-\rangle_{(2i-1)(2i)AB}.
\end{aligned} \tag{27}$$

For the second example, when $\boldsymbol{k_i} = 11$ and $r_{(i)A} = 10$, Alice applies the Pauli operator $\sigma_x\left(= \sigma_{\boldsymbol{k_i}\oplus r_{(i)A}} = \sigma_{10}\right)$ to the qubit $A_{(2i-1)}$ in GHZ-like state of Eq. (25):

$$\begin{aligned}
c_{2i-1}c_{2i} = 00 &: \left[\sigma_x\left|\Psi^{+}\right\rangle_{(2i-1)AB}\right]\left|\Phi^{-}\right\rangle_{(2i)AB} = \left|\Phi^{+}\right\rangle_{(2i-1)AB}\left|\Phi^{-}\right\rangle_{(2i)AB} = |\mathrm{ID}+-\rangle_{(2i-1)(2i)AB},\\
c_{2i-1}c_{2i} = 01 &: \left[\sigma_x\left|\boldsymbol{\Psi^{+}}\right\rangle_{\boldsymbol{(2i-1)AB}}\right]\left|\boldsymbol{\Psi^{+}}\right\rangle_{\boldsymbol{(2i)AB}} = \left|\Phi^{+}\right\rangle_{(2i-1)AB}\left|\boldsymbol{\Psi^{+}}\right\rangle_{\boldsymbol{(2i)AB}} = |\mathrm{Rev}++\rangle_{(2i-1)(2i)AB},\\
c_{2i-1}c_{2i} = 10 &: \left[\sigma_x\left|\Phi^{+}\right\rangle_{(2i-1)AB}\right]\left|\Phi^{-}\right\rangle_{(2i)AB} = \left|\Psi^{+}\right\rangle_{(2i-1)AB}\left|\Phi^{-}\right\rangle_{(2i)AB} = |\mathrm{Rev}+-\rangle_{(2i-1)(2i)AB},\\
\text{or } c_{2i-1}c_{2i} = 11 &: \left[\sigma_x\left|\Phi^{+}\right\rangle_{(2i-1)AB}\right]\left|\boldsymbol{\Psi^{+}}\right\rangle_{\boldsymbol{(2i)AB}} = \left|\Psi^{+}\right\rangle_{(2i-1)AB}\left|\boldsymbol{\Psi^{+}}\right\rangle_{\boldsymbol{(2i)AB}} = |\mathrm{ID}++\rangle_{(2i-1)(2i)AB}.
\end{aligned} \tag{28}$$

For the third example, when $\boldsymbol{k_i} = 11$ and $r_{(i)B} = 10$, Bob applies the Pauli operator $\sigma_x\left(= \sigma_{\boldsymbol{k_i}\oplus r_{(i)A}} = \sigma_{01}\right)$ to the qubit $B_{(2i-1)}$ in GHZ-like state of Eq. (26):

$$\begin{aligned}
c_{2i-1}c_{2i} = 00 &: \left|\Psi^{+}\right\rangle_{(2i-1)AB}\left[\sigma_x\left|\Phi^{-}\right\rangle_{(2i)AB}\right] = \left|\Psi^{+}\right\rangle_{(2i-1)AB}\left|\Psi^{-}\right\rangle_{(2i)AB} = |\mathrm{ID}+-\rangle_{(2i-1)(2i)AB},\\
c_{2i-1}c_{2i} = 01 &: \left|\boldsymbol{\Psi^{+}}\right\rangle_{\boldsymbol{(2i-1)AB}}\left[\sigma_x\left|\boldsymbol{\Psi^{+}}\right\rangle_{\boldsymbol{(2i)AB}}\right] = \left|\Psi^{+}\right\rangle_{(2i-1)AB}\left|\Phi^{+}\right\rangle_{(2i)AB} = |\mathrm{Rev}++\rangle_{(2i-1)(2i)AB},\\
c_{2i-1}c_{2i} = 10 &: \left|\Phi^{+}\right\rangle_{(2i-1)AB}\left[\sigma_x\left|\Phi^{-}\right\rangle_{(2i)AB}\right] = \left|\Phi^{+}\right\rangle_{(2i-1)AB}\left|\Psi^{-}\right\rangle_{(2i)AB} = |\mathrm{Rev}+-\rangle_{(2i-1)(2i)AB},\\
or\ c_{2i-1}c_{2i} = 11 &: \left|\Phi^{+}\right\rangle_{(2i-1)AB}\left[\sigma_x\left|\boldsymbol{\Psi^{+}}\right\rangle_{\boldsymbol{(2i)AB}}\right] = \left|\Phi^{+}\right\rangle_{(2i-1)AB}\left|\Phi^{+}\right\rangle_{(2i)AB} = |\mathrm{ID}++\rangle_{(2i-1)(2i)AB}.
\end{aligned} \tag{29}$$

E3′ Alice and Bob execute the Bell-basis measurements on the qubits $\left\{A_{(2i-1)}, A_{(2i)}\right\}$ and $\left\{B_{(2i-1)}, B_{(2i)}\right\}$ of Eqs. (25) and (26), 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 $2i$). From the first example of phase E2′, if Charlie's measurement outcomes $c_{2i-1}c_{2i} = 01$, the Bell states shared by Alice and Bob are $\left|\Phi^{-}\right\rangle_{(2i-1)AB}\left|\Psi^{+}\right\rangle_{(2i)AB} = |\mathrm{Rev}+-\rangle_{(2i-1)(2i)AB}$ in Eq. (27). Therefore, the Bell-state measurement outcomes $(a_{2i-1}a_{2i}, b_{2i-1}b_{2i})$ of Alice and Bob are as follows:

$$\begin{aligned}
&(00, 11) : \left|\Phi^{+}\right\rangle_{(2i-1)A(2i)A}\left|\Psi^{-}\right\rangle_{(2i-1)B(2i)B}\\
&(01, 10) : \left|\Phi^{-}\right\rangle_{(2i-1)A(2i)A}\left|\Psi^{+}\right\rangle_{(2i-1)B(2i)B}\\
&(10, 01) : \left|\Psi^{+}\right\rangle_{(2i-1)A(2i)A}\left|\Phi^{-}\right\rangle_{(2i-1)B(2i)B}\\
&(11, 00) : \left|\Psi^{-}\right\rangle_{(2i-1)A(2i)A}\left|\Phi^{+}\right\rangle_{(2i-1)B(2i)B}
\end{aligned} \tag{30}$$

Then, they exchange their measurement outcomes $(a_{2i-1}a_{2i}, b_{2i-1}b_{2i})$ in Eq. (30). From the second example of phase E2′, if Charlie' measurement outcomes $c_{2i-1}c_{2i} = 10$, the Bell states shared by Alice and Bob are $|\Psi^+\rangle_{(2i-1)AB}$ $|\Phi^-\rangle_{(2i)AB} = |\text{Rev} + -\rangle_{(2i-1)(2i)AB}$ in Eq. (28). Therefore, the Bell-state measurement outcomes $(a_{2i-1}a_{2i}, b_{2i-1}b_{2i})$ of Alice and Bob are the same as Eq. (30). From the third example of phase E2′, if Charlie's measurement outcomes $c_{2i-1}c_{2i} = 01$, the Bell states shared by Alice and Bob are $|\Psi^+\rangle_{(2i-1)AB}|\Phi^+\rangle_{(2i)AB} = |\text{Rev} + +\rangle_{(2i-1)(2i)AB}$ in Eq. (29). Therefore, the Bell-state measurement outcomes $(a_{2i-1}a_{2i}, b_{2i-1}b_{2i})$ of Alice and Bob are as follows:

$$\begin{aligned}
(00, 10) &: |\Phi^+\rangle_{(2i-1)A(2i)A}|\Psi^+\rangle_{(2i-1)B(2i)B} \\
(01, 11) &: |\Phi^-\rangle_{(2i-1)A(2i)A}|\Psi^-\rangle_{(2i-1)B(2i)B} \\
(10, 00) &: |\Psi^+\rangle_{(2i-1)A(2i)A}|\Phi^+\rangle_{(2i-1)B(2i)B} \\
(11, 01) &: |\Psi^-\rangle_{(2i-1)A(2i)A}|\Phi^-\rangle_{(2i-1)B(2i)B}
\end{aligned} \tag{31}$$

Then, they exchange their measurement outcomes $(a_{2i-1}a_{2i}, b_{2i-1}b_{2i})$ in Eq. (31).
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.
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 to the encrypted authentication key $\boldsymbol{k}_{(i)A} = \boldsymbol{k}_i \oplus \boldsymbol{r}_{(i)A}$ or $\boldsymbol{k}_{(i)B} = \boldsymbol{k}_i \oplus \boldsymbol{r}_{(i)B}$, as presented in Table 4 in [2]. From the first example of phase E3′, because the encrypted authentication key $\boldsymbol{k}_{(i)A} = \boldsymbol{k}_i \oplus \boldsymbol{r}_{(i)A}$ is 10 and $c_{2i-1}c_{2i}$ is 01, the Bell-state measurement outcomes $(a_{2i-1}a_{2i}, b_{2i-1}b_{2i})$ of Alice and Bob must be one of the results of Eq. (30). Note that $\boldsymbol{k}_i = 11$ and $r_{(i)A} = 01$. From the second example of E3′ phase, because the encrypted authentication key $\boldsymbol{k}_{(i)A} = \boldsymbol{k}_i \oplus \boldsymbol{r}_{(i)A}$ is 01 and $c_{2i-1}c_{2i}$ is 10, the Bell-state measurement outcomes $(a_{2i-1}a_{2i}, b_{2i-1}b_{2i})$ of Alice and Bob must also be one of the results of Eq. (30). Note that $\boldsymbol{k}_i = 11$ and $r_{(i)A} = 01$. From the third example of phase E3′, because the encrypted authentication key $\boldsymbol{k}_{(i)B} = \boldsymbol{k}_i \oplus \boldsymbol{r}_{(i)B}$ is 01 and $c_{2i-1}c_{2i}$ is 01, the Bell-state measurement outcomes $(a_{2i-1}a_{2i}, b_{2i-1}b_{2i})$ of Alice and Bob must be one of the results of Eq. (31). Note that $\boldsymbol{k}_i = 11$ and $r_{(i)B} = 10$.

Here, we analyze when the entanglement swapping attacks are applied to these methods. As in the first example, if an authentication key $k_i = 11$ and Alice's random number $r_A = 01$, Alice applies the Pauli operator $i\sigma_y\left(= U_{k_i \oplus r_A}\right)$, which corresponds to an encrypted authentication key $\boldsymbol{k}_{(i)A} = \boldsymbol{k}_i \oplus \boldsymbol{r}_{(i)A} = 10$, to the qubit $(2i-1)A$ in GHZ-like states of Eq. (23), as follows:

$$\begin{aligned}
i\sigma_y|\xi\rangle_{(2i-1)ABC} \otimes |\xi\rangle_{(2i)ABC} = \frac{1}{2}\Big(& |\Phi^-\rangle_{(2i-1)AB}|\Phi^-\rangle_{(2i)AB}|0\rangle_{(2i-1)C}|0\rangle_{(2i)C} \\
& - |\Phi^-\rangle_{(2i-1)AB}|\Psi^+\rangle_{(2i)AB}|0\rangle_{(2i-1)C}|1\rangle_{(2i)C} \\
& + |\Psi^-\rangle_{(2i-1)AB}|\Phi^-\rangle_{(2i)AB}|1\rangle_{(2i-1)C}|0\rangle_{(2i)C}
\end{aligned}$$

$$+ \left|\Psi^{-}\right\rangle_{(2i-1)AB}\left|\Psi^{+}\right\rangle_{(2i)AB}|0\rangle_{(2i-1)C}|1\rangle_{(2i)C}\Big) \tag{32}$$

The GHZ-like states of Eq. (32) are rearranged as follows:

$$\begin{aligned}
&i\sigma_y|\xi\rangle_{(2i-1)ABC}\otimes|\xi\rangle_{(2i)ABC}\\
&=\frac{1}{2}\Big[\big(|\mathrm{ID}++\rangle_{(2i-1)(2i)A(2i-1)(2i)B}+|\mathrm{ID}+-\rangle_{(2i-1)(2i)A(2i-1)(2i)B}\big)\left|\Phi^{+}\right\rangle_{(2i-1)(2i)C}\\
&\quad+\big(|\mathrm{ID}++\rangle_{(2i-1)(2i)A(2i-1)(2i)B}-|\mathrm{ID}+-\rangle_{(2i-1)(2i)A(2i-1)(2i)B}\big)\left|\Phi^{-}\right\rangle_{(2i-1)(2i)C}\\
&\quad-\big(|\mathrm{Rev}+-\rangle_{(2i-1)(2i)A(2i-1)(2i)B}-|\mathrm{Rev}++\rangle_{(2i-1)(2i)A(2i-1)(2i)B}\big)\left|\Psi^{+}\right\rangle_{(2i-1)(2i)C}\\
&\quad-\big(|\mathrm{Rev}+-\rangle_{(2i-1)(2i)A(2i-1)(2i)B}+|\mathrm{Rev}++\rangle_{(2i-1)(2i)A(2i-1)(2i)B}\big)\left|\Psi^{-}\right\rangle_{(2i-1)(2i)C}\Big]
\end{aligned} \tag{33}$$

After Alice and Bob' Bell measurements on $\{(2i)(2i-1)A$ and $(2i)(2i-1)B$ qubits of the GHZ-like states of Eq. (33), Charlie performs a Bell measurement on the $(2i)C$ and $(2i-1)C$ qubits of Eq. (33) without following the E2′ phase. If Alice and Bob's measurement outcomes $(a_{2i-1}a_{2i}, b_{2i-1}b_{2i})$ are $|\mathrm{Rev}+-\rangle_{(2i-1)(2i)A(2i-1)(2i)B}$, Charlie's measurement outcomes $c_{2i-1}c_{2i}$ must be $\left|\Psi^{+}\right\rangle_{(2i-1)(2i)C}$ or $\left|\Psi^{-}\right\rangle_{(2i-1)(2i)C}$. Then, they exchange their measurement outcomes $(a_{2i-1}a_{2i}, b_{2i-1}b_{2i})$. Through these measurement outcomes, Charlie cannot accurately guess that the Pauli operator applied by Alice is σ_x, which corresponds to the encrypted authentication key $\boldsymbol{k}_{(\boldsymbol{i})\boldsymbol{A}}=\boldsymbol{k}_{\boldsymbol{i}}\oplus\boldsymbol{r}_{(\boldsymbol{i})\boldsymbol{A}}=01$, or $i\sigma_y$, which corresponds to the encrypted authentication key $\boldsymbol{k}_{(\boldsymbol{i})\boldsymbol{A}}=\boldsymbol{k}_{\boldsymbol{i}}\oplus\boldsymbol{r}_{(\boldsymbol{i})\boldsymbol{A}}=10$. Note that, Eq. (33) is the same as Eq. (7). Furthermore, as mentioned in Sect. 3, since Eq. (6) and Eq. (33) (= Eq. (7)) differ only in the relative phase ±, it is impossible to distinguish these two equations even if Charlie obtains the measurement outcomes of Alice and Bob. Therefore, Charlie can only estimate the encrypted key $\boldsymbol{k}_{(\boldsymbol{i})\boldsymbol{A}}\in\{01,10\}$ with a 1/2 probability but cannot know the authentication key $k_i=11$. To find out the authentication key $\boldsymbol{k}_{\boldsymbol{i}}$, Charlie should perform phase **E4′ (a)**. Furthermore, in phase **E4′ (a)**, Charlie acts as if it were σ_z-basis measurements rather than Bell measurements as in phase **E2′**. To do this, as Eqs. (27) or (28), Charlie must release the appropriate measurement outcomes. However, Charlie does not know the proper measurement outcomes $c_{2i-1}c_{2i}$ corresponding to Alice and Bob's measurement outcomes $(a_{2i-1}a_{2i}, b_{2i-1}b_{2i})=|\mathrm{Rev}+-\rangle_{(2i-1)(2i)A(2i-1)(2i)B}$. The reason is that even if Charlie knows their outcomes, he still does not know the encrypted authentication key $\boldsymbol{k}_{(\boldsymbol{i})\boldsymbol{A}}\in\{01,10\}$ correctly. Therefore, Charlie cannot guess if his measurement should be $c_{2i-1}c_{2i}=01$ in Eq. (27) or $c_{2i-1}c_{2i}=10$ in Eq. (28). As a result, Charlie's attack is revealed in the final verification phase, **E4′ (b)**.

5 Entanglement swapping attack-resistance CMQEA protocol

In order to the CMQEA protocol to be fundamentally resistant to the entanglement swapping attack described in the above chapter 3, Alice and Bob's measurement

outcomes should be the same even if this attack is performed. Therefore, we propose to use GHZ-like states

$$|\boldsymbol{\xi}\rangle_{(\boldsymbol{2i-1})\boldsymbol{ABC}} \otimes |\boldsymbol{\xi}\rangle_{(\boldsymbol{2i})\boldsymbol{ABC}} = \frac{\mathbf{1}}{\sqrt{\mathbf{2}}}\Big(|\boldsymbol{\Psi}^{+}\rangle_{(\boldsymbol{2i-1})\boldsymbol{AB}}|\mathbf{0}\rangle_{(\boldsymbol{2i-1})\boldsymbol{C}} + |\boldsymbol{\Psi}^{-}\rangle_{(\boldsymbol{2i-1})\boldsymbol{AB}}|\mathbf{1}\rangle_{(\boldsymbol{2i-1})\boldsymbol{C}}\Big) \otimes \frac{\mathbf{1}}{\sqrt{\mathbf{2}}}\Big(|\boldsymbol{\Psi}^{+}\rangle_{(\boldsymbol{2i})\boldsymbol{AB}}|\mathbf{0}\rangle_{(\boldsymbol{2i})\boldsymbol{C}} + |\boldsymbol{\Psi}^{-}\rangle_{(\boldsymbol{2i})\boldsymbol{AB}}|\mathbf{1}\rangle_{(\boldsymbol{2i})\boldsymbol{C}}\Big) \tag{34}$$

as the initial state instead of GHZ-like states in Eq. (1). Note that, Alice and Bob only use two Pauli operators $\sigma_{k_i} \in \{\sigma_0 = I, \sigma_1 = \sigma_z\}$ for an entity authentication. Here, $k_i \in \{0, 1\}$. In this case, even if an untrusted third party executes the entanglement swapping attack, Alice and Bob's measurement outcomes will always be $|\mathbf{Rev} + +\rangle_{(\boldsymbol{2i-1})(\boldsymbol{2i})\boldsymbol{AB}}$ or $|\mathbf{Rev} + -\rangle_{(\boldsymbol{2i-1})(\boldsymbol{2i})\boldsymbol{AB}}$:

$$\begin{aligned}
&|\xi\rangle_{(2i-1)ABC} \otimes |\xi\rangle_{(2i)ABC} \\
&= \frac{1}{2}\Big[\big(|\mathbf{Rev} + +\rangle_{(\boldsymbol{2i-1})(\boldsymbol{2i})\boldsymbol{AB}} + |\mathbf{Rev} + -\rangle_{(\boldsymbol{2i-1})(\boldsymbol{2i})\boldsymbol{AB}}\big)\big|\boldsymbol{\Phi}^{+}\big\rangle_{(\boldsymbol{2i-1})(\boldsymbol{2i})\boldsymbol{C}} \\
&\quad + \big(|\mathbf{Rev} + +\rangle_{(\boldsymbol{2i-1})(\boldsymbol{2i})\boldsymbol{AB}} - |\mathbf{Rev} + -\rangle_{(\boldsymbol{2i-1})(\boldsymbol{2i})\boldsymbol{AB}}\big)\big|\Phi^{-}\big\rangle_{(2i-1)(2i)C} \\
&\quad + \big(|\mathbf{Rev} + +\rangle_{(\boldsymbol{2i-1})(\boldsymbol{2i})\boldsymbol{AB}} + |\mathbf{Rev} + -\rangle_{(\boldsymbol{2i-1})(\boldsymbol{2i})\boldsymbol{AB}}\big)\big|\Psi^{+}\big\rangle_{(2i-1)(2i)C} \\
&\quad + \big(|\mathbf{Rev} + +\rangle_{(\boldsymbol{2i-1})(\boldsymbol{2i})\boldsymbol{AB}} - |\mathbf{Rev} + -\rangle_{(\boldsymbol{2i-1})(\boldsymbol{2i})\boldsymbol{AB}}\big)\big|\Psi^{-}\big\rangle_{(2i-1)(2i)C}\Big]
\end{aligned} \tag{35}$$

As a result, no matter what measurement outcomes $\big|\Phi^{+}\big\rangle_{(2i-1)(2i)C}$, $\big|\Phi^{-}\big\rangle_{(2i-1)(2i)C}$, $\big|\Psi^{+}\big\rangle_{(2i-1)(2i)C}$, and $\big|\Psi^{-}\big\rangle_{(2i-1)(2i)C}$ are obtained by the third party, it is impossible to estimate the secret key $k_i \in \{0, 1\}$. If the security of the protocol is described in terms of information theory, then there is no information Eve can obtain from Alice and Bob's measurements [5]. Therefore, no information leakage occurs in the proposed protocol. For this to work well, Alice and Bob should pre-verify that the third party has shared the GHZ-like states of Eq. (34).

6 Conclusions and Discussion

We described the security of the CMQEA protocol against an entanglement swapping attack by an untrusted third party, Charlie. In particular, we analyzed the possibility of leakage of authentication information when Charlie performs a Bell measurement in the CMQEA protocol. Accordingly, we confirmed that the authentication key sequences could be leaked by untrusted Charlie's entanglement swapping attack with a probability of $1/2^N$. In addition, we described three methods of using the sequence of GHZ-like states, the honesty-checking method, and a random number method to prevent such a threat.

To implement the original CMQEA protocol, GHZ states should be created and Bell-state measurement (BSM) should be performed. Many experimental results for generating GHZ states have been reported [6, 7]. However, when performing BSM based on linear optics, there is a limit in which Bell states $\big|\Phi^{\pm}\big\rangle$ cannot be determined

accurately [8, 9]. As a result, when implementing the CMQEA protocol based on linear optics, there is an error that users cannot be verified with a 50% probability. On the other hand, the CMQEA protocol can be implemented based on nonlinear optics. In this case, the BSM can distinguish all four Bell states, but a decoherence has a significant effect [10, 11]. On the other hand, the improved protocol in Sect. 5 is feasible because of quantum communication protocols that use authentication with only two Bell states $|\Psi^{\pm}\rangle$. Besides, the application of error correction and privacy amplification to this protocol can improve security and practicality [12].

Acknowledgements This work was supported by the NRF programs (2019R1A2C2006381, 2019M3E4A107866011, 2019M3E4A1079777), and the KIST research program (2E30620). C.-H. Hong and H.-J. Yang are supported by the R&D Convergence program of NST (National Research Council of Science and Technology) of Republic of Korea (Grant No. CAP-18-08-KRISS).

References

1. Kang, M.S., Heo, J., Hong, C.H., Yang, H.J., Han, S.W., Moon, S.: Controlled mutual quantum entity authentication with an untrusted third party. Quantum Inf. Process. **17**, 159 (2018)
2. 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)
3. Gao, G., Wang, Y.: Cryptanalysis of controlled mutual quantum entity authentication using entanglement swapping. Commun. Theor. Phys. **67**(1), 33–36 (2017)
4. Wang, Q., Zhang, S., Wang, S., Shi, R.: Comment on "Controlled mutual quantum entity authentication with an untrusted third party". Quantum Inf. Process. (2019). https://doi.org/10.1007/s11128-020-2611-0
5. Liu, Z.H., Chen, H.W.: Analyzing and revising quantum dialogue without information leakage based on the entanglement swapping between any two bell states and the shared secret bell state. Int. J. Theor. Phys. **58**(2), 575–583 (2019)
6. Pan, J.W., Zeilinger, A.: Greenberger–Horne–Zeilinger-state analyzer. Phys. Rev. A **57**, 2208–2211 (1998)
7. Pan, J.W., Daniell, M., Gasparoni, S., Weihs, G., Zeilinger, A.: Experimental demonstration of four-photon entanglement and high-fidelity teleportation. Phys. Rev. Lett. **86**, 4435–4438 (2001)
8. Zhu, F., Zhang, W., Sheng, Y., et al.: Experimental long-distance quantum secure direct communication. Sci. Bull. **62**(22), 1519–1524 (2017)
9. Kim, Y.S., Pramanik, T., Cho, Y., Yang, M., Han, S.W., Lee, S.Y., Kang, M.S., Moon, S.: Informationally symmetrical Bell state preparation and measurement. Opt. Express **26**(22), 29539–29549 (2018)
10. Heo, J., Hong, C.H., Kang, M.S., Yang, H., Yang, H.J., Hong, J.P., Choi, S.G.: Implementation of controlled quantum teleportation with an arbitrator for secure quantum channels via quantum dots inside optical cavities. Sci. Rep. **7**, 14905 (2017)
11. Heo, J., Kang, M.S., Hong, C.H., Choi, S.G., Hong, J.P.: Scheme for secure swapping two unknown states of a photonic qubit and an electron-spin qubit using simultaneous quantum transmission and teleportation via quantum dots inside single-sided optical cavities. Phys. Lett. A **381**, 1845 (2017)
12. Xia, Y., Song, J., Song, H.S.: Quantum dialogue using non-maximally entangled states based on entanglement swapping. Phys. Scr. **76**(4), 363–369 (2007)