




Semi-Quantum Mutual Identity Authentication Using Bell States

ShuQi Jiang^{1,2} · Ri-Gui Zhou^{1,2}  · WenWen Hu^{1,2}

Received: 7 April 2021 / Accepted: 18 July 2021 / Published online: 28 July 2021

© The Author(s), under exclusive licence to Springer Science+Business Media, LLC, part of Springer Nature 2021

Abstract

Identity authentication is an important method to realize information protection in communication. This paper proposes a semi-quantum mutual identity authentication protocol that does not require the third party or complicated operations, only single-qubit measurement operation and XOR operation are performed. The proposed protocol can enable quantum Alice and classical Bob to achieve mutual identity authentication at the same time. The security analysis shows that the proposed protocol can resist the impersonation attack, intercept-measure-resend attack, entangle-measure attack and Trojan horse attack. The comparison demonstrates that our protocol outperforms than other existing protocols in terms of efficiency and performance.

Keywords Semi-quantum authentication · Mutual authentication · Bell states · XOR operation

1 Introduction

Due to the security of quantum information is guaranteed by the characteristics of quantum physics, quantum information has demonstrated higher security than classical information. In recent decades, quantum information is used in various fields, such as quantum machine learning, quantum image processing [1–3] and quantum communication. In the field of quantum communication, Bennet and Brassard [4] proposed the first quantum key distribution protocol in 1984. Subsequently, numerous quantum communication protocols were proposed, including quantum key distribution (QKD) [5–7], quantum secret sharing (QSS) [8–11], quantum secure direct communication (QSDC) [12–14], quantum identity authentication (QIA) [15–31], etc. In 2001, Shor and Preskill [15] proved the unconditional security of quantum key distribution, which established

✉ Ri-Gui Zhou
rgzhou@shmtu.edu.cn

¹ College of Information Engineering, Shanghai Maritime University, Shanghai 201306, China

² Research Center of Intelligent Information Processing and Quantum Intelligent Computing, Shanghai 201306, China

solid foundation for the security of quantum communication. In quantum communication, there may be a forged communicator who pretend to be a legitimate communicator to steal secret information. Therefore, it is imperative to research quantum identity authentication. In 1995, Crépeau and Salvai [16] proposed the first quantum identity authentication protocol. In 1999, Dušek et al. [17] proposed a quantum identity authentication by combining classical identity system and quantum key distribution. Later, a great number of quantum identity authentication protocols were proposed, which can be mainly divided into two categories: quantum identity authentication based on previously shared entangled states [18–20], and quantum identity authentication based on previously shared classical information [21–25]. Since it is difficult to store entanglement states for a long time, most quantum identity authentication protocols are based on sharing classical information in advance. In addition, the third party can be introduced to achieve mutual quantum identity authentication or multi-party quantum identity authentication [26–30]. However, there are very few completely trusted third parties in the real world, the dishonest third party may do evil actions to get secret information [31].

All communicators are quantum parties with complete quantum abilities in quantum communication. But owing to the expensive cost of quantum resources, it is luxury to ensure that all communicators in quantum communication have complete quantum capabilities in reality. In order to reduce the consumption of quantum resources and lower the difficulty of implementation, Boyer et al. [32] proposed the semi-quantum key distribution (SQKD) in 2007, which realized key distribution between quantum communicator and classical communicator. In 2009, Boyer et al. [33] presented two SQKD protocols and proved their complete robustness against attacks.

Combining semi-quantum communication and identity authentication based on pre-shared classical information, Zhou et al. [34] proposed two semi-quantum identification protocols with single photons by using pre-shared classical information in 2019. In Ref. [34], one protocol implements the process of classical Bob authenticates quantum Alice's identity, and in the meantime, another protocol realizes the process of quantum Alice verifies the identity of classical Bob. However, all above-mentioned protocols cannot achieve mutual authentication between quantum Alice and classical Bob. In 2019, Zheng et al. [35] proposed two semi-quantum direct communication protocols based on Bell states, which can realize mutual authentication between quantum Alice and classical Bob. However, there exist two drawbacks in Zheng's protocols: on the one hand, the transmitted secret information is realized through two pre-shared keys, which does not conform the strict definition of QSDC [12, 36]; on the other hand, if the identity authentication is unsuccessful, it is impossible to determine which one is illegal. In addition, the protocols used two classical algorithms to encrypt and reorder particles, which increase the complexity of the protocols. Inspired by the above schemes, a novel semi-quantum mutual authentication protocol is proposed in this paper. Without the third party and the assistance of other classical algorithms, our protocol can achieve the mutual identity authentication between quantum Alice and classical Bob only by using Bell states, simple measurement operation and XOR operation.

The rest of the paper is outlined as follows: in Sect.2, the proposed semi-quantum mutual identity authentication protocol is presented. In Sect.3, the security analysis is depicted. In Sect.4, the efficiency analysis and comparison are presented in detail. Finally, a conclusion is drawn in Sect.5.

2 The Proposed Semi-Quantum Mutual Identity Authentication Protocol

2.1 Basic Idea

The proposed protocol uses two common quantum measurement bases: Z basis and X basis. Here, the measurement property of Bell states is introduced when they are measured in Z basis. Because of the entanglement property of Bell states, after one qubit is measured with the Z basis, the other qubit will collapse to the corresponding state. The correlations of Bell states measured in Z basis are shown in Table 1.

2.2 The Protocol

Suppose that Alice is a powerful quantum communicator, whereas Bob only has classical abilities. Classical Bob is limited to perform following four operations when he accesses a segment of quantum channel: (1) measure: measure the qubit in Z basis ($\{|0\rangle, |1\rangle\}$); (2) prepare: prepare a fresh qubit in Z basis; (3) reflect: reflect the qubit to quantum Alice without disturbance; (4) reorder: reorder the qubits by using different delay lines [32, 33]. Alice and Bob share the classical secret key sequence $K(K_{2i-1}K_{2i} \in \{00, 01, 10, 11\}, i = 1, 2 \dots n)$ in advance by using the SQKD protocol, which had proved to be unconditionally secure [37]. Assume that the quantum channel is noiseless and lossless. To accomplish the mutual authentication between Alice and Bob, the specific steps of the proposed protocol are explained as follows.

Step 1: Preparation.

Alice prepares a sequence of n Bell states, each of which is random in one of the four Bell states $\{|\varphi^+\rangle_{12}, |\varphi^-\rangle_{12}, |\phi^+\rangle_{12}, |\phi^-\rangle_{12}\}$. The subscript 1 represents the first qubit of each state, 2 denotes the second qubit of each state. Alice divides these Bell states into two sequences, the first qubits constitute home sequence $S_H(S_H = \{S_{H1}, S_{H2} \dots S_{Hn}\})$ and the second qubits form traveling sequence $S_T(S_T = \{S_{T1}, S_{T2} \dots S_{Tn}\})$. Alice generates $\frac{n}{2}$ decoy qubits D according to the pre-shared key K . The generation rules are described as:

$$\begin{cases} D_i = |0\rangle \text{ or } |1\rangle, K_{2i-1}K_{2i} \in \{00, 01\} \\ D_i = |+\rangle \text{ or } |-\rangle, K_{2i-1}K_{2i} \in \{10, 11\} \end{cases}, i = 1, 2 \dots \frac{n}{2} \tag{1}$$

Alice inserts D into S_T randomly and obtains sequence S_{TD} . Alice keeps a record of the inserted positions and initial states of these decoy qubits, and then, she sends S_{TD} to Bob.

Table 1 The correlations of Bell states measured in Z basis

Bell states	The measurement result of one qubit	The measurement result of the other qubit
$ \varphi^\pm\rangle = \frac{1}{\sqrt{2}}(00\rangle \pm 11\rangle)$	$ 0\rangle$ $ 1\rangle$	$ 0\rangle$ $ 1\rangle$
$ \phi^\pm\rangle = \frac{1}{\sqrt{2}}(01\rangle \pm 10\rangle)$	$ 0\rangle$ $ 1\rangle$	$ 1\rangle$ $ 0\rangle$

Step 2: Eavesdropping detection.

After receiving the sequence S_{TD} , Bob informs Alice that he has received S_{TD} . Alice announces the inserted positions of the decoy qubits. Alice and Bob perform corresponding operations on the decoy qubits according to the pre-shared key sequence K , respectively.

If $K_{2i-1}K_{2i} \in \{00, 01\}$, Bob measures the decoy qubits D_i in the Z basis and publishes the corresponding measurement results.

If $K_{2i-1}K_{2i} \in \{10, 11\}$, Bob reorders the decoy qubits D_i and reflects them to Alice. After receiving all the reflected decoy qubits, Alice asks Bob for the original order and restores. Alice measures them in X basis afterwards.

Alice compares all measurement results with all initial states of the decoy qubits. If the measurement results are different from the initial states, the protocol will be restarted from beginning; otherwise, Bob can obtain sequence S_T and go to the next step.

Step 3: Measurement.

Alice and Bob perform Z basis measurement on the qubits at the corresponding positions of S_H and S_T . After the measurement, the measurement results are converted into classical results R_A and R_B . The conversion rules are shown in Table 2.

Step 4: XOR operation.

Alice announces the initial states of prepared Bell states. Based on the Z basis measurement results in step 3 and the initial Bell states announced by Alice, Bob can deduce the Z basis measurement results of Alice as R_A^* . In the same way, Alice can deduce the Z basis measurement results of Bob as R_B^* . Bob performs bitwise XOR on R_A^* and K , R_B and K to obtain I_A^* and I_B . Similarly, Alice can get I_A and I_B^* . The detailed operations are explained as Eq. (2). Bob sends I_A^* to Alice and Alice sends I_B^* to Bob.

$$\begin{cases} R_{Ai} \oplus K_i = I_{Ai}, I_{Ai} = \{I_{A1}, I_{A2} \dots I_{An}\} \\ R_{Bi} \oplus K_i = I_{Bi}, I_{Bi} = \{I_{B1}, I_{B2} \dots I_{Bn}\} \\ R_{Ai}^* \oplus K_i^* = I_{Ai}^*, I_{Ai}^* = \{I_{A1}^*, I_{A2}^* \dots I_{An}^*\} \\ R_{Bi}^* \oplus K_i^* = I_{Bi}^*, I_{Bi}^* = \{I_{B1}^*, I_{B2}^* \dots I_{Bn}^*\} \end{cases}, (i = 1, 2 \dots n) \tag{2}$$

Step 5: Authentication.

If $I_A = I_A^*$, Alice successfully authenticates Bob, the identity of Bob is legal; otherwise, Bob is the illegal communicator.

If $I_B = I_B^*$, Bob successfully authenticates Alice, the identity of Alice is legal; otherwise, Alice is the illegal communicator.

Table 2 The classical results of single qubit measured in Z basis

Z basis measurement result	Classical result
$ 0\rangle$	0
$ 1\rangle$	1

3 Security Analysis

Assumed that the attacker Eve has strong quantum capabilities. Eve can access quantum channel and execute the evil actions to steal secret information. In this section, we analyze four different attack strategies and verify that the proposed protocol is immune to these attacks.

3.1 Impersonation Attack

If the attacker Eve impersonates Alice, he will try to complete fake authentication by randomly preparing qubits, sending qubit sequence, and performing single-qubit measurement. Since Eve is ignorant of the pre-shared key sequence K , Eve can only randomly generate the decoy qubits $D_e (D_e \in \{|0\rangle, |1\rangle, |+\rangle, |-\rangle\})$. The probability that each decoy qubit generated correctly by Eve is $\frac{1}{4}$. Consider that when Eve prepares the decoy qubit in wrong basis, the probability that legitimate communicator can get the correct measurement result is $\frac{1}{4} \times \frac{1}{2} + \frac{1}{4} \times \frac{1}{2} = \frac{1}{4}$. Thus Eve has $\frac{1}{4} + \frac{1}{4} = \frac{1}{2}$ probability to escape from the detection without being detected. In other words, there are $\frac{n}{2}$ decoy qubits suffering from Eve's attack, then Eve's attack can be detected with probability $P_1 = 1 - (\frac{1}{2})^{\frac{n}{2}}$. From Fig. 1, if n is large enough, P_1 is approximate to 1. Therefore, when the number of decoy qubits is large enough, it is difficult for Eve to pass the eavesdropping detection.

If the attacker Eve pretends to be Bob, he will unable to perform proper operation on the corresponding qubits in the sequence S_{TD} because of the absence of the pre-shared key sequence K . Eve chooses correct operation with probability $\frac{1}{2}$. If Eve chooses wrong operation, the probability that legitimate communicator can get correct measurement result is $\frac{1}{2} \times \frac{1}{2} = \frac{1}{4}$. Then Eve can pass the eavesdropping detection with probability $\frac{1}{2} + \frac{1}{4} = \frac{3}{4}$. Therefore, there are $\frac{n}{2}$ decoy qubits suffering from Eve's attack, then Eve's attack can be detected with probability $P_2 = 1 - (\frac{3}{4})^{\frac{n}{2}}$. From Fig. 2, if n is large enough, P_2 is approximate to 1. When the number of decoy qubits is large enough, it is difficult for Eve to pass the eavesdropping detection.

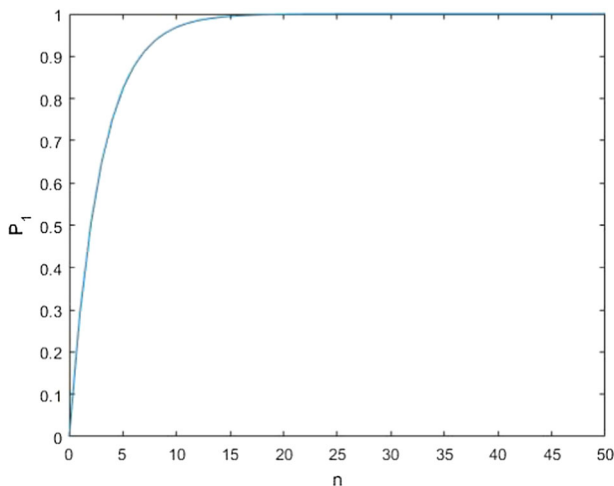


Fig. 1 The detection probability of Eve impersonating Alice

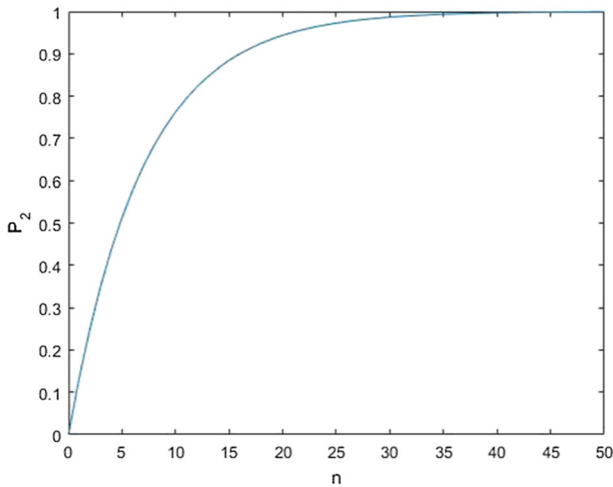


Fig. 2 The detection probability of Eve impersonating Bob

More importantly, even if Eve, which impersonated a legitimate user, passed the eavesdropping detection by chance, he still unable to perform the correct XOR operation in the final authentication stage without the pre-shared key sequence K and his existence would be noticed. So Eve cannot complete a fake authentication with impersonation attack.

3.2 The Intercept-Measure-Resend Attack

In the intercept-measure-resend attack, the attacker Eve intercepts the sequence S_{TD} sent by Alice to Bob in step 1, Eve measures each qubit in S_{TD} , and prepares a fake sequence of ancillary qubits $E(E \in \{|0\rangle, |1\rangle, |+\rangle, |-\rangle\})$ according to the measurement results. Then Eve sends the fake sequence E to Bob. In step 3, Eve intercepts the qubits returned by Bob to Alice, measures these qubits and attempts to obtain operation information performed by Bob. However, Eve doesn't know the inserted positions and initial states of the decoy qubits, and Eve chooses the measurement basis randomly. The decoy qubits are not all mutually orthogonal, and Eve cannot know the states of the decoy qubits with certainty via his measurement. The probability that Eve chooses the correct measurement basis to measure the decoy qubit is $\frac{1}{2}$, and at the meantime, when he measures the decoy qubit in wrong basis, the probability that legal communicator can get the correct measurement result is $\frac{1}{2} \times \frac{1}{2} = \frac{1}{4}$. Thus, Eve has $\frac{1}{2} + \frac{1}{4} = \frac{3}{4}$ probability to pass the eavesdropping detection. There are $\frac{n}{2}$ decoy qubits suffering from Eve's attack, therefore, the probability that Eve can be detected by legitimate communicators is $P_3 = 1 - \left(\frac{3}{4}\right)^{\frac{n}{2}}$. It is the same as P_2 , so as n is large enough, then P_3 tends to 1. Alice and Bob can easily detect the existence of Eve in the eavesdropping detection. In addition, Bob reorders the decoy qubits before returning them to Alice, no one except Bob knows the original order. Therefore, Eve is unable to obtain any useful information from the intercept-measure-resend attack.

3.3 The Entangle-Measure Attack

In the entangle-measure attack, when the traveling qubit is sent from Alice to Bob, the attacker Eve entangles the traveling qubit with an ancillary qubit $|e\rangle$ by a unitary operation U_e , which will produce the results in Eq. (3).

$$\begin{aligned}
 U_e|0\rangle &|e\rangle = a|0\rangle|e_{00}\rangle + b|1\rangle|e_{01}\rangle \\
 U_e|1\rangle &|e\rangle = c|0\rangle|e_{10}\rangle + d|1\rangle|e_{11}\rangle \\
 U_e|+\rangle &|e\rangle = \frac{1}{2} \left[|+\rangle(a|e_{00}\rangle + b|e_{01}\rangle + c|e_{10}\rangle + d|e_{11}\rangle) \right. \\
 &\quad \left. + |-\rangle(a|e_{00}\rangle - b|e_{01}\rangle + c|e_{10}\rangle - d|e_{11}\rangle) \right] \\
 U_e|-\rangle &|e\rangle = \frac{1}{2} \left[|+\rangle(a|e_{00}\rangle + b|e_{01}\rangle - c|e_{10}\rangle - d|e_{11}\rangle) \right. \\
 &\quad \left. + |-\rangle(a|e_{00}\rangle - b|e_{01}\rangle - c|e_{10}\rangle + d|e_{11}\rangle) \right]
 \end{aligned} \tag{3}$$

where $|a|^2 + |b|^2 = |c|^2 + |d|^2 = 1$. Then Eve lets the traveling qubit go on its way. After transmission, Eve measures ancillary qubit to get Bob’s operations. In order to pass the eavesdropping detection without introducing any errors, Eq. (3) must satisfy the following conditions:

$$\begin{cases}
 b|e_{01}\rangle = c|e_{10}\rangle = 0 \\
 a|e_{00}\rangle - b|e_{01}\rangle + c|e_{10}\rangle - d|e_{11}\rangle = 0 \\
 a|e_{00}\rangle + b|e_{01}\rangle - c|e_{10}\rangle - d|e_{11}\rangle = 0
 \end{cases} \tag{4}$$

As a result, it is easy to find that $a|e_{00}\rangle = d|e_{11}\rangle$, which means that Eve cannot differentiate $|e_{00}\rangle$ between $|e_{11}\rangle$. In step 1, the decoy qubits D are randomly inserted into the sequence S_T , Eve doesn’t know the inserted positions and initial states of D . Furthermore, Bob reorders the decoy qubits before returning to Alice, Eve is unaware of the original order. Eve cannot obtain any valuable information from the ancillary qubit. Therefore, Eve fails to extract operation information with the entangle-measure attack.

3.4 The Trojan Horse Attack

Since our protocol is a two-way communication protocol, the attacker Eve may implement the Trojan horse attack to get secret information. The Trojan horse attack can be generally divided into two types, i.e., the invisible photon eavesdropping (IPE) attack and the delay photon Trojan horse attack. In order to avoid these attack strategies, Alice and Bob need to place wavelength filters and photon number splitters before devices [38–40].

4 The Efficiency Analysis and Comparison

Cabello [41] proposed the efficiency definition of quantum and semi-quantum communication protocols, as $\eta = \frac{b_s}{q_t + b_t} \times 100\%$, where b_s , q_t and b_t represent the number of useful quantum bits and classical bits, the number of total qubits and the number of total classical bits. Considering the qubits used for eavesdropping detection, $q_t = q_c + d$, where q_c means the number of qubits used for transmitting authentication information and d means the number of qubits used for eavesdropping detection.

To accomplish mutual authentication between quantum Alice and classical Bob, the number of useful qubits and classical bits $b_s = n + n + n + n = 4n$. Alice and Bob need to exchange classical information, the number of total classical bits $b_t = n + n = 2n$. Alice prepares $\frac{n}{2}$ decoy qubits for the eavesdropping detection, thus the number of qubits used for eavesdropping detection $d = \frac{n}{2}$. The number of qubits used for transmitting authentication information $q_c = n + n = 2n$. From the above analysis, we can know the protocol efficiency will be $\eta = \frac{4n}{2n + \frac{n}{2} + 2n} \times 100\% = 88.9\%$.

In Ref. [34], Zhou et al. proposed two protocols for classical Bob to authenticate quantum Alice and quantum Alice to authenticate classical Bob respectively, but the mutual authentication of quantum Alice and classical Bob cannot be realized at the same time. In Ref. [25], quantum Alice and quantum Bob achieved mutual authentication simultaneously with the assistance of a third party. Nonetheless, the trusted third party hardly exists in the real world. In Ref. [35], in the process of realizing QSDC, quantum Alice and classical Bob accomplished mutual authentication meanwhile, but the protocol did not satisfy the strict definition of QSDC [12, 36], and two classical algorithms are used to assist mutual authentication, which are more complicated. Besides, when the authentication fails, it is impossible to determine whether the identity of Alice or Bob is illegal. Compared with these protocols, the protocol proposed in this paper reduces the use of quantum resources, without the existence of the third party, mutual authentication can be accomplished only by performing simple measurement operation and XOR operation. Even if the authentication fails, the illegal identity of communicators can be distinguished. More importantly, the efficiency of our protocol is improved compared with protocol in Ref. [35].

5 Conclusion

In this paper, a semi-quantum mutual identity authentication protocol is proposed based on Bell states. The security of the proposed protocol has been explicitly analyzed. Security analysis indicates that our protocol is secure against four common attacks. Compared with some existing protocols, the proposed protocol reduces the use of quantum resources and does not need the third party or complex operations. It achieves the mutual authentication simultaneously between quantum Alice and classical Bob only through simple measurement operation and XOR operation. In addition, the existence of illegal communicator can also be detected.

Acknowledgements This work is supported by the Shanghai Science and Technology Project in 2020 under Grant No.20040501500.

Authors' Contributions ShuQi Jiang and Ri-Gui Zhou conceived the theory and designed the protocol. ShuQi Jiang wrote the paper and contributed security analysis.

Declarations

Conflict of interest The authors declare that there is no conflict of interest.

References

1. Li, Y.C., Zhou, R., Xu, R.Q., Luo, J., Jiang, S.X.: A quantum mechanics-based framework for EEG signal feature extraction and classification. *IEEE Trans. Emerg. Top. Comput.* 14, (2020)
2. Li, Y., Zhou, R.-G., Xu, R., Luo, J., Hu, W.: A quantum deep convolutional neural network for image recognition. *Quant Sci. Technol.* 5, 44003 (2020)

3. Hu, W.W., Zhou, R.G., El-Rafei, A., Jiang, S.X.: Quantum image watermarking algorithm based on Haar wavelet transform. *IEEE Access*. **7**, 121303–121320 (2019)
4. Bennett, C.H., Brassard, G.: Quantum cryptography: public key distribution and coin tossing. *Theor. Comput. Sci.* **560**, 7–11 (2014)
5. WANG, X., HU, J.: Quantum key distribution with the decoy-state method. *Sci. Sin. Phys. Mech. Astron.* **41**, 459–465 (2011)
6. Hwang, W.Y.: Quantum key distribution with high loss: toward global secure communication. *Phys. Rev. Lett.* **91**, (2003)
7. Wu, J.Z., Yan, L.: Quantum Key Distribution Protocol Based on GHZ Like State and Bell State. *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*. 12240 LNCS, 298–306 (2020)
8. Tong, X., Wen, Q.Y., Zhu, F.C.: Quantum secret sharing based on GHZ states entanglement swapping. *Beijing Youdian Daxue Xuebao/J Beijing Univ. Posts Telecommun.* **30**, 44–48 (2007)
9. Tan, X., Jiang, L.: Improved three-party quantum secret sharing based on bell states. *Int. J. Theor. Phys.* **52**, 3577–3585 (2013)
10. Abulkasim, H., Hamad, S., Khalifa, A., El Bahnasy, K.: Quantum secret sharing with identity authentication based on bell states. *Int. J. Quantum Inf.* **15**, 6–8 (2017)
11. Zhou, R.-G., Huo, M., Hu, W., Zhao, Y.: Dynamic multiparty quantum secret sharing with a trusted party based on generalized GHZ state. *IEEE Access*. **9**, 22986–22995 (2021)
12. Deng, F.G., Long, G.L., Liu, X.S.: Two-step quantum direct communication protocol using the Einstein-Podolsky-Rosen pair block. *Phys. Rev. A - At. Mol. Opt. Phys.* **68**(6), (2003)
13. Wang, C., Deng, F.G., Li, Y.S., Liu, X.S., Long, G.L.: Quantum secure direct communication with high-dimension quantum superdense coding. *Phys. Rev. A - At. Mol. Opt. Phys.* **71**, 1–4 (2005)
14. Yu, C.H., De Guo, G., Lin, S.: Quantum secure direct communication with authentication using two nonorthogonal states. *Int. J. Theor. Phys.* **52**, 1937–1945 (2013)
15. Shor, P.W., Preskill, J.: Simple proof of security of the BB84 quantum key distribution protocol. *Phys. Rev. Lett.* **85**, 441–444 (2000)
16. Crépeau, C., Salvai, L.: Quantum oblivious mutual identification. *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*. 921, 133–146 (1995)
17. Dušek, M., Haderka, O., Hendrych, M., Myška, R.: Quantum identification system. *Phys. Rev. A - At. Mol. Opt. Phys.* **60**, 149–156 (1999)
18. Shi, B., Li, J., Liu, J., Fan, X., Guo, G.: Quantum key distribution and quantum authentication based on entangled state. *Phys. Lett. A* 281 83–87. 281, 83–87 (2001)
19. Míhara, T.: Quantum identification schemes with entanglements. *Phys. Rev. A - At. Mol. Opt. Phys.* **65**(4), (2002)
20. Li, X., Chen, L.: Quantum Authentication Protocol Using Bell State. In: *The First International Symposium on Data, Privacy, and E-Commerce (ISDPE 2007)*. pp. 128–132 (2007)
21. Zhang, Z., Zeng, G., Zhou, N., Xiong, J.: Quantum identity authentication based on ping-pong technique for photons. *Phys. Lett. Sect. A Gen. At. Solid State Phys.* **356**, 199–205 (2006)
22. Yuan, H., Liu, Y., Min, P.G., Zhu, Z.G., Zhou, J., Zhang, Z.J.: Quantum identity authentication based on ping-pong technique without entanglements. *Quantum Inf. Process.* **13**, 2535–2549 (2014)
23. Hong, C.H., Heo, J., Jang, J.G., Kwon, D.: Quantum identity authentication with single photon. *Quantum Inf. Process.* **16**, 1–20 (2017)
24. Zawadzki, P.: Quantum identity authentication without entanglement. *Quantum Inf. Process.* **18**, 1–12 (2019)
25. Zhang, S., Chen, Z.K., Shi, R.H., Liang, F.Y.: A novel quantum identity authentication based on bell states. *Int. J. Theor. Phys.* **59**, 236–249 (2020)
26. Yang, Y.G., Wen, Q.Y., Zhang, X.: Multiparty simultaneous quantum identity authentication with secret sharing. *Sci. China, Ser. G Physics, Mech. Astron.* **51**, 321–327 (2008)
27. Yu-Guang, Y., Qiao-Yan, W.: Economical multiparty simultaneous quantum identity authentication based on Greenberger–Horne–Zeilinger states. *Chinese Phys. B.* **18**, 3233–3237 (2009)
28. Kang, M.S., Hong, C.H., Heo, J., Lim, J.I., Yang, H.J.: Controlled mutual quantum entity authentication using entanglement swapping. *Chinese Phys. B.* **24**, 090306 (2015)
29. Penghao, N., Yuan, C., Chong, L.: Quantum authentication scheme based on entanglement swapping. *Int. J. Theor. Phys.* **55**, 302–312 (2016)
30. Naseri, M.: Revisiting quantum authentication scheme based on entanglement swapping. *Int. J. Theor. Phys.* **55**, 2428–2435 (2016)
31. 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**, 1–15 (2018)

32. Boyer, M., Kenigsberg, D., Mor, T.: Quantum key distribution with classical bob. *Phys. Rev. Lett.* **99**, 1–5 (2007)
33. Boyer, M., Gelles, R., Kenigsberg, D., Mor, T.: Semiquantum key distribution. *Phys. Rev. A - At. Mol. Opt. Phys.* **79**, 1–12 (2009)
34. Zhou, N.R., Zhu, K.N., Bi, W., Gong, L.H.: Semi-quantum identification. *Quantum Inf. Process.* **18**, 1–17 (2019)
35. Tao, Z., Chang, Y., Zhang, S., Dai, J., Li, X.: Two semi-quantum direct communication protocols with mutual authentication based on bell states. *Int. J. Theor. Phys.* **58**, 2986–2993 (2019)
36. Rong, Z., Qiu, D., Zou, X.: Semi-quantum secure direct communication using entanglement. *Int. J. Theor. Phys.* **59**, 1807–1819 (2020)
37. Krawec, W.O.: Security of a semi-quantum protocol where reflections contribute to the secret key. *Quantum Inf. Process.* **15**, 2067–2090 (2016)
38. Deng, F.-G., Zhou, P., Li, X.-H., Li, C.-Y., Zhou, H.-Y.: Robustness of two-way quantum communication protocols against Trojan horse attack. *Physics*. 3–5 (2005)
39. Deng, F.G., Li, X.H., Zhou, H.Y., Zhang, Z.J.: Erratum: improving the security of multiparty quantum secret sharing against Trojan horse attack. *Phys. Rev. A - At. Mol. Opt. Phys.* **73**(49901), (2006)
40. Cai, Q.Y.: Eavesdropping on the two-way quantum communication protocols with invisible photons. *Phys. Lett. Sect. A Gen. At. Solid State Phys.* **351**, 23–25 (2006)
41. Cabello, A.: Quantum key distribution in the Holevo limit. *Phys. Rev. Lett.* **85**, 5635–5638 (2000)

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.