International Journal of Theoretical Physics (2021) 60:265–273
https://doi.org/10.1007/s10773-020-04688-7

Authenticated Semi-Quantum Secret Sharing Based on GHZ-Type States

Aihan Yin[1] · Tong Chen[1]

Received: 4 September 2020 / Accepted: 14 December 2020 / Published online: 10 January 2021

Abstract

As is known to all that entities authentication can provides secure communication for QSS protocol. In this paper, the authors propose a novel semi-quantum secret sharing (SQSS) scheme where identity authentication is adopted to verify the identification of partners in communication based on GHZ-type states. Any related quantum operations can be performed by the quantum Alice, however, classical partners can only perform classical operations on the transmitted qubits as well as unitary transformation. In addition, the paper also shows that the protocol is secure resist some eavesdropping attacks.

Keywords Semi-quantum secret sharing · Identity authentication · GHZ-type states

1 Introduction

Quantum cryptography is a new discipline that combines quantum physics with cryptography, which is a new cryptographic structure that can implement quantum cryptography by applying quantum physics, and it mainly involves the quantum key distribution (QKD) [1, 2], quantum identity authentication (QIA) [3, 4], quantum secure direct communication (QSDC) [5, 6] and quantum secret sharing (QSS) [7–9], etc. The fundamental idea of QSS is that the sender Alice can split a secret message into several parts and sends them to every receiver so that the secret message can not be restructured by each of the individual. QSS has three intentions: distributing secret keys, sharing classical secret messages and sharing quantum secrets (unknown quantum states) among amount of parties. In 1999, Hillery et al. [7] proposed the first QSS protocol that can safely share secret information by using three-particle GHZ entangled states as a quantum resource. However, existing QSS protocols require users to have full quantum capabilities. Obviously, it is unrealistic that each participant has the high quantum resource and preparation or measuring of the capability of an arbitrary quantum state. To resolve these problems, Boyer et al. [10] first put forward the concept of a semi-quantum cryptography scheme based on the BB84 protocol in 2007. Then in 2009, Boyer et al. [11] further improved the semi-quantum concept by using single

✉ Tong Chen
759063946@qq.com

[1] Department of Information Engineering, East China Jiao Tong University, Jiangxi, 330013, China

photons as quantum resources. Since then, semi-quantum idea has been applied to different quantum information processing work, such as semi-quantum key distribution (SQKD) [12, 13], semi-quantum secure direct communication (SQSDC) [14] and semi-quantum secret sharing (SQSS) [15–17] etc. Moreover, the introduction of the idea of semi-quantum into QSS makes the QSS protocol more easily to be implemented in the actual systems while saving quantum resources. The characteristics of SQSS has been constantly attracting scholars to study and discuss in-depth, and now there are many valuable research results has been acheived. In 2010, Li et al. [15] put forward to two SQSS schemes by using maximally entangled GHZ states, only one of which has all quantum capabilities. In 2016, Gao et al. [17] presented a multi-party SQSS scheme by using Bell states as quantum resources.

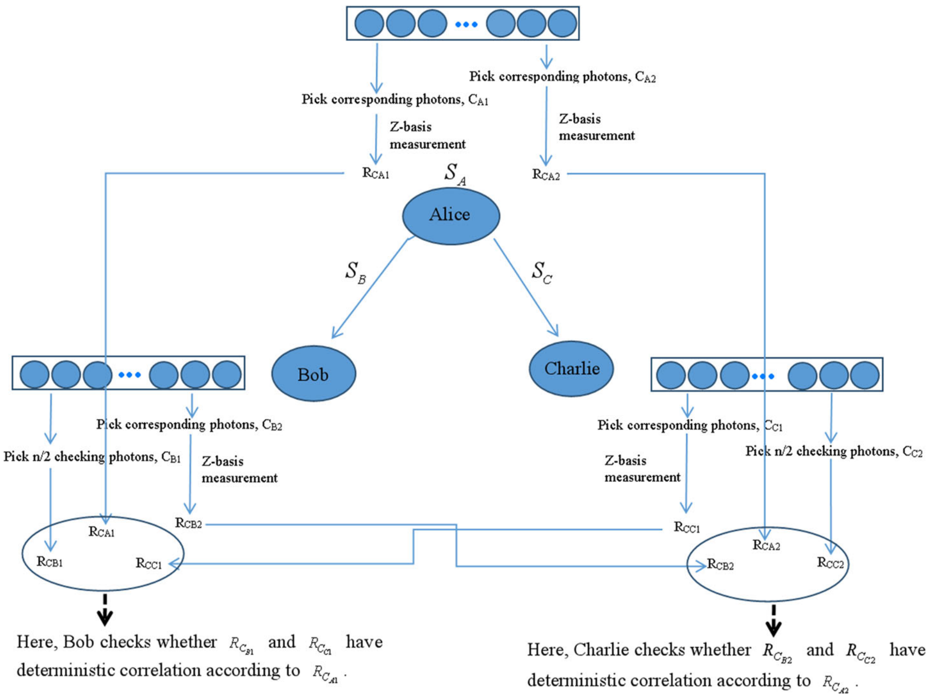
Furthermore, identity authentication can provide secure communication for QSS protocol. It is the procedure of verifying the identification of partner in communication, to protect a communication from malicious attacker pretending to be a legitimate partner. In 2004, Nguyen [18] proposed a quantum dialogue (QD) protocol to achieve the process of quantum identity authentication, in which the sender and the receiver can exchange their secret message simultaneously. Since then, many QD protocols have been proposed [19–21].

Based on the above analysis, the authors realized that although the previous SQSS protocol could withstand most attacks, eavesdroppers may still launch special attacks provided that the user does not verify the identity of the other party during the security check. Thus the authors proposed a new SQSS scheme in which two classical partners Bob and Charlie, can simultaneously perform mutual identity authentication by using three-particle entangled states (GHZ-type states). The idea of entities authentication in the proposed QSS scheme was inspired by the protocols in Ref. [22]. The difference between our protocol and the protocol in Ref. [10] is that in the authors' protocol, the classical Bob and Charlie can also apply the classical unitary transformation $U \in \{I, x, y, z\}$ (where I is a 2×2 unit matrix, x, y, z are the usual Pauli matrices) on the qubits respectively. It's well-known that they construct a complete basis of any 2×2 matrices. And the authors' protocol is more efficient than the previous protocol. Finally, the result shows that the proposed SQSS scheme can efficiently resist intercept-resend attack, modification attack and Trojan horse attack.

The rest of this paper is organized as follows: In Section 2, we proposed a SQSS scheme based on GHZ-type states. In Section 3, we gave an example to further explain our scheme. In Section 4, we analyzed the security of the scheme from multiple angles. In Section 5, the proposed SQSS scheme is comprehensively compared with other existing schemes. Finally, Section 6 we drew the conclusion.

2 The Proposed SQSS Scheme

Assume that the sender Alice wants to share a secret with two classical agents Bob and Charlie. The protocol includes two phases: the first phase is identity authentication phase and the second one is SQSS phase. In the first phase, a QD protocol is considered between Bob and Charlie for authenticating the identity of each other similar as Ref. [18]. The difference between the protocol and the protocol in Ref. [10] is that Alice prepares N GHZ-type states, she takes each particle from each state to form three ordered sequences S_A, S_B, S_C. Alice sends S_B sequence to Bob, and sends S_C sequence to Charlie, then Bob and Charlie can use the measurement result of Alice to determine the initial states of the Bell states in the identity authentication phase. In the second phase, Alice shares a message among Bob and Charlie. The proposed protocol proceeds in the following steps (See Fig. 1):


Pick corresponding photons, C_{A2}
Pick corresponding photons, C_{A1}
Z-basis measurement
Z-basis measurement
R_{CA1}
S_A
R_{CA2}
Alice
S_B
S_C
Bob
Charlie
Pick corresponding photons, C_{B2}
Pick n/2 checking photons, C_{B1}
Z-basis measurement
Pick corresponding photons, C_{C1}
Pick n/2 checking photons, C_{C2}
Z-basis measurement
R_{CB2}
R_{CA1}
R_{CB1}
R_{CC1}
R_{CC1}
R_{CA2}
R_{CB2}
R_{CC2}

Here, Bob checks whether $R_{C_{B1}}$ and $R_{C_{C1}}$ have deterministic correlation according to $R_{C_{A1}}$.

Here, Charlie checks whether $R_{C_{B2}}$ and $R_{C_{C2}}$ have deterministic correlation according to $R_{C_{A2}}$.

Fig. 1 The proposed scheme

Step 1 Alice generates N three-particle GHZ-type entangled states, and each one is in the state:

$$|\phi_0\rangle = \frac{1}{\sqrt{2}}(|+++\rangle + |---\rangle)_{ABC} = \frac{1}{\sqrt{2}}\left(|0\rangle \frac{(|00\rangle + |11\rangle)}{\sqrt{2}} + |1\rangle \frac{(|10\rangle + |01\rangle)}{\sqrt{2}}\right)_{ABC}$$

Where subscript A represents the 1st particle of each state, B describe as the 2nd particles of each state, and C represents the 3rd particles of each state. She divides these states into three ordered sequences of qubits:$S_A = \{A_1, A_2, \cdots, A_N\}$, $S_B = \{B_1, B_2, \cdots, B_N\}$, $S_C = \{C_1, C_2, \cdots, C_N\}$. Then Alice sends sequence S_B, S_C to Bob and Charlie respectively, and retains the quantum sequence S_A for herself.

Step 2 After receiving S_B from Alice, Bob informs Alice that she has received the S_B. Bob randomly selects n_1 $(n_1 < N/2)$ qubits from the received sequence S_B as the checking state, called C_{B1}, and then informs Alice the positions of C_{B1} via a public classical channel. Once the position of C_{B1} is received, Alice selects the particle composition sequence C_{A1} at the corresponding position in S_A, and using Z-basis $\{|0\rangle, |1\rangle\}$ to measure C_{A1} to obtain the measurement result $R_{C_{A1}}$. Then, Alice sends $R_{C_{A1}}$ to Bob through the public classic channel. According to the $R_{C_{A1}}$, Bob can deduce whether the particle B and particle C at the corresponding positions are in state $\left|\varphi^+\right\rangle = \frac{(|00\rangle+|11\rangle)}{\sqrt{2}}$ or $\left|\psi^+\right\rangle = \frac{(|01\rangle+|10\rangle)}{\sqrt{2}}$. Then Bob randomly chooses one of the four unitary operations $\{U_{00}, U_{01}, U_{10}, U_{11}\}$, to be applied on C_{B1}. Next, the position of C_{B1} will be announced to Charlie.

Step 3 According to the positions announced from Bob, Charlie chooses the corresponding photons in S_C, called C_{C1}, and measures C_{C1} using Z-basis $\{|0\rangle, |1\rangle\}$ to obtain the measurement result, $R_{C_{C1}}$. Charlie also selects n_1 ($n_1 < N/2$) photons as checking photons, called C_{C2}, from the remaining S_C. Charlie announces the positions of C_{C2} to Alice. Alice takes the action similar to step 2 to choose the corresponding photons in S_A, called C_{A2}, and measures C_{A2} using Z-basis $\{|0\rangle, |1\rangle\}$ to obtain the measurement result, $R_{C_{A2}}$. Then Alice sends $R_{C_{A2}}$ to Charlie via a public classical channel. Upon receiving the $R_{C_{A2}}$, according to Alice's measurement result being 0 or 1, Charlie can determine that particle B and particle C in the corresponding entangled state collapse into entangled state $\left|\varphi^+\right\rangle = \frac{(|00\rangle+|11\rangle)}{\sqrt{2}}$ or $\left|\psi^+\right\rangle = \frac{(|01\rangle+|10\rangle)}{\sqrt{2}}$, and randomly applies one of the four unitary operations $\{U_{00}, U_{01}, U_{10}, U_{11}\}$ on C_{C2}. Finally, Charlie sends $R_{C_{C1}}$ and announces the positions of C_{C2} to Bob.

Step 4 Upon receiving measurement result $R_{C_{C1}}$ and the positions of C_{C2}, Bob first measures C_{B1} using Z-basis $\{|0\rangle, |1\rangle\}$ to obtain the measurement result $R_{C_{B1}}$. Then, Bob checks whether $R_{C_{B1}}$ and $R_{C_{C1}}$ have deterministic correlation according to $R_{C_{A1}}$, as follows. If the i^{th} bit of $R_{C_{A1}}$ is 0, the i^{th} bit of $R_{C_{C1}}$ and $R_{C_{B1}}$ are the same, otherwise, the result of the i^{th} bit of $R_{C_{C1}}$ and $R_{C_{C1}}$ is opposite, where $i = 1, 2, \cdots, n_1$. If it exists correlation, Bob trusts there is no eavesdropper during the transmission of S_B and simultaneously the identity of Alice is authenticated. Otherwise, they stop this communication. Subsequently, Bob selects the corresponding photon in the remaining sequence S_B, called C_{B2}, according to the position of C_{C2}, and uses the Z-basis $\{|0\rangle, |1\rangle\}$ to measure C_{B2} to obtain the measurement result $R_{C_{B2}}$. Finally, Bob sends $R_{C_{B2}}$ to Charlie through the public classic channel.

Step 5 Upon receiving measurement result $R_{C_{B2}}$, Charlie first measures C_{C2} to obtain the measurement result $R_{C_{C2}}$. Then, Alice checks whether $R_{C_{C2}}$ and $R_{C_{B2}}$ have deterministic correlation according to $R_{C_{A2}}$. Similar to step 4, if it exists correlation, Charlie trusts there is no eavesdropper during the transmission of S_C and simultaneously the identity of Bob is authenticated. Otherwise, they stop this communication. After that, sequences S_A, S_B and S_C remove the authenticated particles, and the remaining sequences convert to S'_A, S'_B and S'_C, respectively.

Step 6 Next, Alice shares the secret message with Bob and Charlie using S'_B and S'_C.

(i) Bob randomly selects particles in S'_B to measure with Z-basis and prepares new identical quantum states to send to Alice (called SHARE); or Bob returns the particles without any interference (called CHECK). The resent qubits are reordered via different delay lines. At the same time, Charlie does the action similar to Bob. It is important to note that at least one particle in the same position in S'_B and S'_C is measured by both Bob and Charlie, and if there is no such photon, the scheme will be aborted and restarted.

(ii) Alice receives and restores the qubits reflected by Bob and Charlie in quantum memory, and announces that she has received their reflected particles publicly. Alice asks Bob and Charlie to announce the actions they take on each particle and the order of the particles.

(iii) For each particle in S'_A, Alice will take four different ACTIONs according to the actions performed by Bob and Charlie, as illustrated in Table 1.

ACTION 1: *Alice measures her own qubit in the Z-basis* $\{|0\rangle, |1\rangle\}$.

Table 1 Alice's action on the particles of checking state

Bob's action	Charlie's action	Alice's action
SHARE	SHARE	ACTION 1
SHARE	CHECK	ACTION 2
CHECK	SHARE	ACTION 3
CHECK	CHECK	ACTION 4

ACTION 2: *Alice combines her qubit with Charlie's reflected qubit and performs a Bell measurement.*

ACTION 3: *Alice combines her own qubit with Bob's reflected qubit and performs a Bell measurement.*

ACTION 4: *Alice combines her own qubit with the two reflected qubits and performs an appropriate three-particle measurement.*

(iv) Alice evaluates the probability of error. If the probability exceeds the preset threshold, then the communication step terminates. Otherwise, the protocol continues. Bob can work with Charlie to get the Shared key:

$$S = R_B \oplus R_C$$

Here R_B, R_C represent the measurement results of Bob and Charlie respectively. $\oplus$ represents the XOR operation.

3 An Example

In this section, the authors give an example to show our scheme.

Assume the sequence generated by Alice is $\{|\phi\rangle_1, |\phi\rangle_2, |\phi\rangle_3, |\phi\rangle_4, |\phi\rangle_5, |\phi\rangle_6, |\phi\rangle_7, |\phi\rangle_8\}$. Alice takes each particle from each state to form three ordered sequences $S_A = \{a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8\}$, $S_B = \{ b_1, b_2, b_3, b_4, b_5, b_6, b_7, b_8\}$, $S_C = \{ c_1, c_2, c_3, c_4, c_5, c_6, c_7, c_8\}$. Alice sends S_B sequence to Bob, and sends S_C sequence to Charlie. After receiving S_B, we can assume that Bob randomly selects $n_1 = 3$ ($n_1 < 4$) qubits in S_B to form checking sequence $C_{B1} = \{ b_1, b_2, b_3 \}$, and then Bob announces the positions of C_{B1} to Alice. Alice takes the corresponding qubits to form $C_{A1} = \{ a_1, a_2, a_3 \}$ and measures each selected qubits in Z-basis. Assume that the measurement result $R_{C_{A1}} = \{ 0, 0, 1 \}$ and Bob takes unitary operations U_{00}, U_{11}, U_{10} on C_{B1}, then the state of corresponding particle B and particle C is $\{ |\varphi\rangle_1^+, |\varphi\rangle_2^+, |\psi\rangle_3^+ \}$. Bob informs Charlie the positions of C_{B1}. Charlie selected the corresponding particles in S_C to form $C_{C1} = \{c_1, c_2, c_3\}$, and measured them with Z-basis to get the measurement results $R_{C_{C1}}$ and then Charlie randomly selects $n_2 = 3$ ($\mathrm{n}_2 < 4$) qubits in remaining sequence S_C to form checking sequence $C_{C2} = \{ c_4, c_5, c_6 \}$. Assume that $R_{C_{A2}} = \{ 1, 1, 0 \}$, the unitary operations of Charlie is U_{11}, U_{01}, U_{00}. Then Charlie sends $R_{C_{C1}}$ and the positions of C_{C2} to Bob. Next, Bob authenticates the identity of Charlie. If it is valid, Bob sends $R_{C_{B2}}$ to Charlie. Charlie authenticates the identity of Bob, and then Alice shares the secret message with Bob and Charlie using $S'_B = \{ \mathrm{b}_7, \mathrm{b}_8\}$ and $S'_C = \{ c_7, c_8\}$. If only the 8th particle is measured by both Bob and Charlie and $R_{B8} = 1$, $R_{C8} = 0$, remaining photon is for checking. Finally, Bob and Charlie can get $S = 1$ according to $S = R_{B8} \oplus R_{C8}$.

4 Security Analysis

In this section, the authors analyze the security of the proposed SQSS protocol. There are three probability attacks: (1) intercept-resend attack; (2) Modification attack; (3) Trojan horse attack. The outside attacks are much less threatening than internal attacks because dishonest participants already know shadows of the secret. Therefore, in the following security analysis, the authors focus on the attack of the internal dishonest participants. Suppose Bob is a dishonest participant in the proposed SQSS scheme.

4.1 Intercept-Resend Attack

In the proposed SQSS scheme, dishonest participant, Bob can know the positions of C_{C2} and sends the measurement result $R_{C_{B2}}$ to Charlie. Alice also sends the measurement result $R_{C_{A2}}$ to Charlie. When dishonest participant Bob adopts a intercept-and-resend attack, there are two potential scenarios:

(i) In identity authentication phase, Bob intercepts $R_{C_{A2}}$ and re-sends a new sequence composed of $|0\rangle$ and $|1\rangle$ to Charlie. He can get the corresponding states of particle B and particle B. However, he will be detected in Step 5, because Bob does not know the unitary operations $U_{xy} = \{U_{00}, U_{01}, U_{10}, U_{11}\}$, which Charlie takes on the particle C. The probability for Bob to know the right unitary operation is $1/4$, but the probability for Bob to finish the identity authentication is $1/2$, and the reason is that when Charlie chooses U_{00} and U_{01}, the results that Bob prepares are the same and when Charlie chooses U_{10} and U_{11}, the results that Bob prepares are the same. Consequently, the probability of detecting Bob's attack is $1 - \left(\frac{1}{2}\right)^{n2}$, If n_2 is large enough, the probability of detecting Bob's attack is 1.

(ii) In SQSS phase, Bob intercepts S_C and re-sends a new sequence S_E randomly composed of $|0\rangle$ and $|1\rangle$ to Charlie and then Bob intercepts $R_{C_{A2}}$ and re-sends a new sequence composed of $|0\rangle$ and $|1\rangle$ to Charlie. He can get the corresponding states of particle B and particle C. However, he will be detected in Step 5, because Bob does not know the unitary operations $U_{xy} \in \{U_{00}, U_{01}, U_{10}, U_{11}\}$, which Charlie takes on the particles in S_E. The probability for dishonest participant Bob to finish the identity authentication is 1/2. Consequently, the probability of detecting Bob's attack is $1 - \left(\frac{1}{2}\right)^{n2}$, If n_2 is large enough, the probability of detecting Bob's attack converges to 1. Accordingly, the proposed SQSS scheme is secure against intercept-resend attack.

4.2 Modification Attack

In the modification attack, the attacker eve deliberately modified the content of the transmitted photon, so that the correspondent could obtain a false or wrong key message without being discovered. In the identity authentication phase, Eve can perform unitary operations on the particles in the sequence S_C, so as to modify the particles held by Charlie without being detected. After receiving $R_{C_{A2}}$, Charlie can know each state of corresponding particle B and particle C. Undoubtedly, Charlie will detect Eve in step 5. Since Charlie knows the $R_{C_{A2}}$ and $R_{C_{B2}}$, he measures sequence C_{C2}, expecting that $R_{C_{C2}}$ and $R_{C_{B2}}$have deterministic correlation. In the SQSS phase, Eve can perform unitary operations on the particles in the sequence S'_C, so as to modify the particles held by Charlie without being detected. However, Alice knows initial states, after she received the sequence sent from Bob and Charlie, Eve will be detected. Therefore, the proposed SQSS scheme can resist modification attack efficiently.

4.3 Trojan Horse Attack

In the SQSS scheme, the dishonest participant, Bob, can attach some invisible photons to each particle of S_C transmitted from Alice to Charlie, and inserting some delay photons in the same time window to each particle of S_C. By adding a wavelength filter (WF) before all devices and a photon number splitter (PNS) [23, 24], it can resist the attack.

5 Performance Evaluation and Comparisons

In the section, comparisons are made between the proposed QSS scheme and the schemes in Refs. [15, 26] and [27–31]. Table 2 show the comparison results, in which the information-theoretical efficiency [25] is defined as $\eta = b_s/q_t + b_t$, where b_s denotes the secret information bits transmitted, q_t denotes the total qubits used ($q_t = q_c + d$ Where q_c denotes the number of qubits used to simultaneously send messages and d denotes the number of qubits used for checking sequence.) and b_t denotes the classical bits exchanged between Alice and Bob.

5.1 Comparison with Ref. [15]

Li et al. [15] proposed a semi-quantum secret sharing scheme based on entangled states, which showed that Alice shared secrets with two classic parties by using the maximum entangled GHZ state. Behind the perfect scheme, however, there is an attack threat that cannot be defended against the Trojan horse attack. Compared with Li et al.'s scheme, in the autors' scheme, in order to detect Trojan horse attacks, Alice (Bob) can use wavelength filter (WF) to remove the hidden photons and consume decoy photons in photon splitting (PNS) to detect delayed photons. In addition, the authors did not insert decoy particles as safety detection particles.

5.2 Comparison with Ref. [26]

Tsai et al. [26] proposed a semi-quantum secret sharing scheme based on the W states, which uses the characteristics of semi-quantum to reduce the consumption of quantum resources. Although this scheme improves the efficiency of qubits, there is a security problem of dishonest participants. In other words, the efficiency of qubits is improved at the expense of

Table 2 Comparison of the proposed scheme with other schemes

Protocols	η	Quantum states used	Semi-quantum	Identity authentication
Ref.[15]	1/12	GHZ state	Yes	No
Ref.[26]	1/8	W state	No	No
Ref.[28]	1/4	Bell state	Yes	No
Ref.[31]	2/11	Two particle entangled States	Yes	No
Our protocol	1/4	GHZ type state	Yes	Yes

security. In our proposal, the authors introduce quantum identity authentication technology to comprehensively improve the efficiency of qubits under the premise of ensuring the security.

5.3 Comparison with Refs. [27–31]

Based on the EPR states proposed by Gao et al. [28] aimed at the efficient multi-party quantum secret sharing protocol, Hwang et al. [27] pointed out that this protocol had a low utilization rate of qubits. Therefore, Hwang et al. proposed a multi-partied quantum secret sharing protocol based on the GHZ states, which effectively solved the problem of qubit utilization. Later, Liu et al. found that the protocol proposed by Hwang et al. had security loopholes. Therefore, Liu et al. [29] proposed an improved scheme to detect the presence of eavesdroppers by inserting a single photon to deceive it. After that, Xie et al. [30] applied the semi-quantum technology to the quantum secret protocol and proposed a novel semi-quantum secret sharing scheme. Subsequently, Yin et al. [31] continued to improve based on the scheme of Xie et al. and made a phased contribution to improving the efficiency and safety of qubits.

Communication security is an eternal topic for mankind. Based on the advantages and disadvantages of the previous scheme, the authors innovatively proposed a semi-quantum secret sharing scheme based on identity authentication technology. Compared with the previous one, the authors' scheme has perfectly applied the identity authentication technology to the SQSS scheme. It enables to resist the various attacks to prevent the information leakage thus ensure the security of communication.

6 Conclusions

In this paper, the authors have proposed an authenticated SQSS protocol based on GHZ-type sates. Before sharing the secret message, participant Bob and Charlie has performed mutual authentication with each other. Eventually, the participants Bob and Charlie perform the XOR operation to deduce Alice's sharing secret. Simultaneously, it shows that the proposed SQSS protocol can efficiently resist intercept-resend attack, modification attack and Trojan horse attack. In addition, since the proposed SQSS protocol does not require all participants to have quantum capabilities, secret sharing can be achieved at a lower cost. Performance evaluation shows that the qubits efficiency is higher than most existing schemes.

Acknowledgements This work is supported by the National Natural Science Foundation of China under Grant No. 61762039.

References

1. Shor, P.W., Preskill, J.: Simple Proof of Security of the BB84 Quantum Key Distribution Protocol. Phys. Rev. Lett. **85**(2), 441–444 (2000)
2. Margarida, P., Go, K., Akihiro, M., et al.: Quantum key distribution with correlated sources. Science advances. **37**(6) (2020)
3. Chang, H., Jino, H., Jin, G.J.: Quantum identity authentication with single photon. Quantum Inf. Process. **16**(10), 236 (2017)
4. Zhang, S., et al.: A novel quantum identity authentication based on Bell states. Int. J. Theor. Phys. **59**(1), 236-249 (2020)

5. Zhang, W., et al.: Quantum Secure Direct Communication with Quantum Memory. Phys. Rev. A.**118**(22), 220501 (2017)
6. Cai, J., Pan, Z., Wang, T.J., et al.: High-capacity quantum secure direct communication using hyper-entanglement of photonic qubits. Int. J. Theor. Phys. **14**(8) (2016)
7. Hillery, M., Buoek, V., Berthiaume A.: Quantum secret sharing. Phys. Rev. A. **59**(3), 1829-1834 (1999)
8. Qin, H.W., Dai, Y.: Efficient quantum secret sharing. Quantum Inf. Process. **15**(5), 2091–2100 (2016)
9. Deng, F.G., et al.: Efficient high-capacity quantum secret sharing with two-photon entanglement. Phys. Lett. A. **372**(12), 1957-1962 (2008)
10. Boyer, M., Kenigsberg, D., Mor, T.: Quantum key distribution with classical bob. Phys. Rev. Lett. **99**(14), 140501 (2007)
11. Boyer, M., Gelles, R., Kenigsberg, D., et al.: Semi-quantum key distribution. Phys. Rev. A. **79**(3), 32341-32341 (2009)
12. Zhu, K.N., Zhou, N.R., Wang, Y.Q., et al.: Semi-Quantum Key Distribution Protocols with GHZ States. Int. J. Theor. Phys. **57**(6) (2018)
13. Zhou, N.R., Zhu, K.N., Zou, X.F.: Multi-Party Semi-Quantum Key Distribution Protocol With Four-Particle Cluster States. Annalen Der Physik. **531**(8) (2019)
14. Zou, X.F., Qiu, D.W.: Three-Step semi-quantum secure direct communication protocol. Science China Phys. Mech Astron. **57**(9), 1696-1702 (2014)
15. Li, Q., Chan, W.H., Long, D.Y.: Semi-quantum secret sharing using entangled states. Phys. Rev. A. **82**(2), 2422-2427 (2010)
16. Lin, J., Yang, C.W., Tsai, C.W., Hwang, T.: Intercept-resend attacks on semi-quantum secret sharing and the improvements. Int. J. Theor. Phys. **52**(1), 156-162 (2013)
17. Gao, G., Wang, Y., Wang, D.: Multiparty semiquantum secret sharing based on rearranging orders of qubits. Mod. Phys. Lett. B. **30**, 10 (2016)
18. Nguyen, B.A.: Quantum dialogue. Phys. Rev. A. **328**(1), 6-10 (2004)
19. Shi, G.F., Xi, X.Q., Hu, M.L., et al.: Quantum secure dialogue by using single photons. Opt. Commu. **283**(9), 1984-1986 (2010)
20. Shen, D., Ma, W., Yin, X., et al.: Quantum Dialogue with Authentication Based on Bell States. Int. J. Theor. Phys. **52**(6), 1825-1835 (2013)
21. Yin, A.H., Lin, W.B., Fan., P.: Controlled quantum dialogue scheme based on different unspecific two-particle entangled state. Mod. Phys. Lett. A. **35**(2),175-179 (2019)
22. Lin, C.Y., Yang, C.W., Hwang, T.: Authenticated Quantum Dialogue Based on Bell States. Int. J. Theor. Phys. **54**(3),780-786 (2015)
23. Li, X.H., Deng, F.G., Zhou, H.Y.: Improving the security of secure direct communication based on the secret transmitting order of particles. Phys. Rev. A, **74**(5) (2006)
24. Zheng, T., Zhang, S., Gao, X., et al.: Practical quantum private query based on Bell state. Mod. Phys. Lett. A. **74**(24), 592 (2019)
25. Cabello, A.: Quantum key distribution in the Holevo limit. Phys. Rev. Lett. **85**(26), 5635-8 (2000)
26. Tsai, C.W., Yang, C.W., Lee, N.Y.: Semi-quantum secret sharing protocol using w-state. Mod. Phys. Lett. A. **34**(27), 1950213 (2019)
27. Hwang, T., Hwang, C.C., Li, C.M.: Multiparty quantum secret sharing based on GHZ states. Phys. Scr. **83**, 045004 (2011)
28. Gao, G.: Multiparty quantum secret sharing using two-photon three-dimensional Bell states. Commun. Theor. Phys. **52**, 421-4 (2009)
29. Liu, X.F., Pan, R.J.: Cryptanalysis of quantum secret sharing based on GHZ states. Phys. Scr. **84**(4), 045015 (2011)
30. Xie, C., Li, L.Z., Qiu, D.W.: A Novel Semi-Quantum Secret Sharing Scheme of Specific Bits. Int. J. Theor. Phys. **54**(10), 3819-3824 (2015)
31. Yin, A.H., Tong, Y.: A novel semi-quantum secret sharing scheme using entangled states. Mod. Phys. Lett. B. **32**(22) (2018)

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