frontiers in Physics

TYPE Original Research
PUBLISHED 23 March 2026
DOI 10.3389/fphy.2026.1806357

OPEN ACCESS

EDITED BY
Q. H. Liu,
Hunan University, China

REVIEWED BY
Tian Yuan,
Beijing University of Posts and Telecommunications (BUPT), China
Chongqiang Ye,
Hangzhou City University, China

*CORRESPONDENCE
Jun-Yao Liu,
332416010926@zzuli.edu.cn

RECEIVED 07 February 2026
REVISED 04 March 2026
ACCEPTED 10 March 2026
PUBLISHED 23 March 2026

CITATION
Cui J-T, Liu J-Y, Xin X-J, Li C-Y, Li F-G and Zhang L (2026) Efficient semi-quantum dialogue protocol using single-photon.
Front. Phys. 14:1806357.
doi: 10.3389/fphy.2026.1806357

Efficient semi-quantum dialogue protocol using single-photon

Jian-Tao Cui[1], Jun-Yao Liu[1]*, Xiang-Jun Xin[1], Chao-Yang Li[1], Fa-Gen Li[2] and Ling Zhang[1]

[1]College of Software Engineering, Zhengzhou University of Light Industry, Zhengzhou, China, [2]School of Computer Science and Engineering, University of Electronic Science and Technology of China, Chengdu, China

Semi-quantum dialogue (SQD) enables secure bidirectional communication even when one participant has limited quantum capabilities. In order to solve the problems of low efficiency and quantum resource constraints, an efficient SQD protocol using single-photon is proposed. In the SQD, one communicating party needs to have semi-quantum capabilities to complete the dialogue, which could consume lower quantum resource. Moreover, single photons as quantum channels significantly reduces both preparation and operational costs. Finally, decryption can be performed without any classical disclosure, effectively preventing potential information leakage. Security analysis demonstrates resilience against common attacks, including intercept-resend, measure-resend, entanglement-measurement, and Trojan horse attacks, with no information leakage. Compared with existing semi-quantum dialogue protocols, our proposed protocol consumes fewer quantum resources while achieving higher communication efficiency and enhanced security.

KEYWORDS

decoy particle, information entropy, quantum communication efficiency, semi-quantum dialogue, single photons

1 Introduction

Quantum communication, a fundamental branch of quantum information science, exploits the uncertainty principle of quantum mechanics to achieve secure communication between distant parties. In 1984, Bennett and Brassard first proposed the quantum key distribution (QKD) protocol [1]. Motivated by the success of QKD, extensive researches have been conducted within quantum information science, such as quantum secret sharing (QSS) [2–4], quantum secure direct communication (QSDC) [5–7] and quantum dialogue (QD) [8–10]. Although QD is developed on the basis of QSDC, significant differences exist between these two communication schemes. QSDC directly transmits secret messages over a quantum channel, typically in a one-way manner. Building on this idea, QD enables the simultaneous two-way exchange of secret messages within a single protocol. However, QD is not equivalent to two rounds of QSDC, as both parties jointly encode their messages on shared quantum states, resulting in distinct protocol structures and security properties.

Nguyen first formulated the concept of QD in 2004 [8], where Bell states were employed for encoding and decoding. Subsequently, extensive research on quantum dialogue has been conducted, leading to the development of several important branches. Among them, controlled quantum dialogue (CQD) [11] achieves equal information exchange between the two parties through a controller, simplifies the entanglement preparation process, and enhances security through hash verification. Measurement-device-independent quantum dialogue (MDI-QD) [12] allows both communicating parties to prepare quantum states while an untrusted third party performs the measurements,

ensuring security without requiring quantum memory and providing inherent resistance to memory attacks.

However, most quantum communication protocols still require substantial quantum resources, which hinders the practical deployment of QD protocols. To mitigate this issue, Boyer et al. introduced semi-quantum key distribution (SQKD) in 2007 [13], restricting one participant to classical operations while the other retains full quantum capabilities. Building upon SQKD principles, the first semi-quantum dialogue (SQD) protocol was subsequently proposed [14], which introduces a unified framework of semi-quantum protocols using Bell states, further reducing implementation costs by allowing one party to perform only limited classical operations. Since then, more SQD protocols have been developed. In 2018, Ye et al. proposed two SQD protocols [15] based on single photons, one of which does not require the classical party to possess measurement capabilities, thereby effectively enhancing the flexibility of the protocol. Furthermore, both of the proposed protocols achieve a communication efficiency of 66.7%.

Later, Pan proposed a SQD protocol based on Bell states in 2020 [16], where secure and reliable encoding and exchange of information are achieved through the entanglement collapse of the Bell states. In addition, the classical one-time pad encryption process further improves the security of the protocol. However, a security flaw in Pan's SQD protocol based on Bell states allows an undetected double controlled-NOT attack. To address this issue, Shi proposed an improved and secure protocol [17] in 2023. In the same year, Shi proposed a SQD protocol using hyperentangled Bell states [18]. Unlike previous SQD protocols, this protocol combines the advantages of SQKD and SQD, introducing a new mode of dialogue and providing a new way of thinking. In 2025, Yang et al. designed a SQD protocol based on GHZ states [19], the protocol does not employ decoy particles and delay-line operations, effectively reducing the overhead for the classical party. In the same year, Li et al. proposed a SQD protocol based on four-particle Ω state [20]. By utilizing the properties of Ω state, the protocol effectively facilitates the exchange of classical information between two parties.

However, on the one hand, the above SQD protocols using single photons require the disclosure of classical messages for decryption, which inevitably affects their efficiency. On the other hand, those SQD protocols using entangled states still suffer from low efficiency and difficulties for the hard prepared entangled-state. In the proposed SQD protocol, Bob encrypts his message using the single-photon sequence sent by Alice, which fundamentally differentiates it from QSDC.

To address these limitations, we propose an efficient semi-quantum dialogue protocol using single-photon. The proposed protocol offers several advantages:

1. The protocol employs single photons as quantum resources, offering easier preparation and higher transmission efficiency than the QD protocols with entangled states;
2. The semi-quantum communicating party can only perform classical operations, thereby reducing the quantum device requirements;
3. The SQD protocol does not require the disclosure of any classical information related to decryption.

The remainder of this manuscript is organized as follows. Section 2 introduces the detailed procedure of the proposed protocol. Section 3 presents the detailed security analysis. Section 4 evaluates the efficiency and compares the proposed protocol with existing protocols. Finally, Section 5 provides the conclusions.

2 Protocol description

The SQD protocol using single-photon involves two participants: the fully quantum party, Alice, who possesses complete quantum capabilities, and the semi-quantum party, Bob, who is limited to performing only a restricted set of operations. They use single photons as the quantum channel for transmitting secret information. The operations available to the semi-quantum party can be classified into the following two modes:

A. Detection mode
   i. Measuring the qubits in the Z-basis $\{|0\rangle, |1\rangle\}$;
   ii. Preparing the (fresh) qubits in the Z-basis;
   iii. Sending or reflecting the qubits without disturbance.
B. Communication mode
   i. Preparing the (fresh) qubits in the Z-basis;
   ii. Reordering the qubits (via different delay lines);
   iii. Sending or reflecting the qubits without disturbance.

The efficient semi-quantum dialogue protocol using single-photon is described as follows.

2.1 Initialization stage

1. Step 1: Alice and Bob send a binary bit string of length N to each other respectively, denoted as $M_A = \left\{m_a^j | 1 \le j \le N\right\}$, $M_B = \left\{m_b^j | 1 \le j \le N\right\}$, where $m_a^j, m_b^j \in \{0,1\}$.
2. Step 2: Alice and Bob share $2N$ classical bits $K_{AB} = \left\{k_{ab}^i | 1 \le i \le 2N\right\}$, where $k_{ab}^i \in \{0,1\}$. The distribution of "0" and "1" in K_{AB} is uniform and each accounts for half.
3. Step 3: Alice and Bob share the hash function $H: \{0,1\}^* \rightarrow \{0,1\}^n$. The preparation rule of the information particle state R is: $|0\rangle$ corresponds to secret information "0", $|1\rangle$ corresponds to secret information "1".

2.2 Encryption stage

1. Step 1: Alice's process of initial state preparation and encoding. Alice selects all the bits with a value of "0" in the key sequence K_{AB} to form the information particle sequence $K_0 = \left\{k_0^j | 1 \le j \le N\right\}$, where $k_0^j = 0$; correspondingly, Alice selects all the bits with a value of "1" in the key sequence K_{AB} to form the decoy photon sequence $K_1 = \left\{k_1^j | 1 \le j \le N\right\}$, where $k_1^j = 1$. Similarly, Bob also formed sequences K_0 and K_1 in the same way. For each bit k_{ab}^i in K_{AB}, if $k_{ab}^i = 0$, Alice prepares the information particle s_a^j based on her secret information m_a^j and the rule R, and eventually forms the sequence $S_A = \left\{s_a^j | 1 \le j \le N\right\}$, then she records the position of each $k_{ab}^i = 0$ in K_{AB}; if $k_{ab}^i = 1$, Alice randomly prepares a decoy photon d_a^j from four states $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$ and records its initial state. The final sequence is formed as $D_A = \left\{d_a^j | 1 \le j \le N\right\}$, and Alice records the position of each $k_{ab}^i = 1$ in K_{AB}. Alice combines sequences S_A and D_A into sequence $S_A' = \left\{s_a^{i\prime} | 1 \le i \le 2N\right\}$

based on the positions of $k_{ab}^{i}=0$ and $k_{ab}^{i}=1$ in K_{AB}. The possible particles corresponding to each bit k_{ab}^{i} in the key sequence K_{AB} are shown in Table 1. To further illustrate Alice's specific operations, Figure 1 presents an encoding method executed by Alice. Then Alice prepares a new decoy particle sequence $D_{AB}=\left\{d_{ab}^{j}|1\le j\le N\right\}$, where d_{ab}^{j} from four states $\{|0\rangle,|1\rangle,|+\rangle,|-\rangle\}$ and randomly inserts into the sequence $S_A{}'$. She sends the inserted sequence $S_A{}''$ to Bob.

2. Step 2: The first round of eavesdropping detection. Alice and Bob can install a photon number splitter and wavelength filter in front of their device to prevent the attack of the Trojan horse. After Bob receives the inserted sequence $S_A{}''$, Alice announces the position of the decoy particle sequence D_{AB}. At this moment, Bob can perform the operations in Detection mode. Then he divides the sequence into $S_A{}'$ and D_{AB}, for each d_{ab}^{j} in D_{AB}, Bob randomly selects a Z-basis measurement and, based on the outcome, prepares the same state in the Z-basis. Alternatively, he may simply allow the particle to reflect without introducing any disturbance. After confirming that Alice has received all the particles, Bob discloses his operations and collaborates with Alice to jointly calculate the error rate. When the error rate is lower than the threshold previously negotiated by both parties, Step 3 is executed. Otherwise, the communication will be terminated.
3. Step 3: Bob's Encryption Process. After confirming the channel security, for each $s_a^{i}{}'$ in $S_A{}'$, Bob distinguishes whether it belongs to S_A or D_A based on K_{AB}. For each s_a^{j} in S_A, Bob performs a Z-basis measurement, records the measurement result $m_a^{j}{}'$, and deduces Alice's secret information M_A. At this moment, Bob can perform the operations in Communication mode. Then, based on his own secret information m_b^{j} and the rule R, Bob prepares the information particle s_b^{j} in the Z-basis to form the particle sequence $S_B=\left\{s_b^{j}|1\le j\le N\right\}$, and replaces s_a^{j}. For each d_a^{j} in D_A, Bob records it as sequence $D_B=\left\{d_d^{j}|1\le j\le N\right\}$. Alice and Bob calculate $H_A=H(M_A)$ based on M_A using the hash function H and compare whether the measurement results are consistent. If both parties calculate the same value of H_A, the protocol will proceed; otherwise, it will be terminated. Using the delay line, Bob rearranges all the particles in S_B and D_B based on Alice's secret information M_A: If $m_a^{j}=0$, Bob does not perform any operation on particles d_b^{j} and s_b^{j}; if $m_a^{j}=1$, Bob swaps the positions of particles d_b^{j} and s_b^{j} and records the swapped positions. Bob forms new sequences $\overline{S_B}$ and $\overline{D_B}$, then he merges sequences $\overline{S_B}$ and $\overline{D_B}$ into sequence $S_B{}'=\left\{s_b^{i}{}'|1\le i\le 2N\right\}$ based on the positions of $k_{ab}^{i}=0$ and $k_{ab}^{i}=1$ in K_{AB}. Later he sends $S_B{}'$ to Alice and use the classical channel to send the rearrangement rules to Alice. To further illustrate Bob's specific operations, Figure 2 presents one possible operation that Bob might perform.
4. Step 4: The second round of eavesdropping detection. After Alice receives $S_B{}'$, she decomposes sequence $S_B{}'$ into $\overline{S_B}$ and $\overline{D_B}$ based on the positions of $k_{ab}^{i}=0$ and $k_{ab}^{i}=1$ in K_{AB}. Then she restores S_B and D_B based on M_A, and performs corresponding basis measurements on the particles in D_B. If the error rate is lower than the threshold set by both parties in advance, Step 5 is executed; otherwise, the communication will be terminated.

TABLE 1 Alice's encryption and the particles corresponding to $S_A{}'$.

k_{ab}^{i}	m_a^{j}	$s_a^{i}{}'\left(s_a^{j}\right)$	$s_a^{i}{}'\left(d_a^{j}\right)$
0	0	$\|0\rangle$	-
	1	$\|1\rangle$	-
1	-	-	$\|0\rangle,\|1\rangle,\|+\rangle,\|-\rangle$

5. Step 5: Alice decrypts Bob's secret information. Alice performs Z-basis measurements on the particles in S_B, eventually obtaining Bob's secret information M_B. Alice and Bob calculate $H_B=H(M_B)$ based on M_B using the hash function H and compare whether the measurement results are consistent. If the H_B values calculated by both parties are identical, the decrypted message M_B is considered valid; otherwise, it is deemed invalid. The communication process is completed.

To facilitate understanding of the encoding and decoding processes of the protocol, a simplified example (excluding security check) is provided as follows:

Assume that the shared key K_{AB} between Alice and Bob is 101100, Alice's secret message M_A is 101, and Bob's secret message M_B is 110. Based on K_{AB}, Alice may prepare the following initial sequence and send it to Bob: $S_A{}''=\left\{|+\rangle_{D_A}|1\rangle_{D_{AB}}|1\rangle_{S_A}|1\rangle_{D_A}|0\rangle_{D_{AB}}|-\rangle_{D_A}|+\rangle_{D_{AB}}|0\rangle_{S_A}|1\rangle_{S_A}\right\}$, wherein the information particle sequence $S_A=\left\{|1\rangle_{S_A}|0\rangle_{S_A}|1\rangle_{S_A}\right\}$, the decoy photon sequence $D_A=\left\{|+\rangle_{D_A}|1\rangle_{D_A}|-\rangle_{D_A}\right\}$, and $D_{AB}=\left\{|1\rangle_{D_{AB}}|0\rangle_{D_{AB}}|+\rangle_{D_{AB}}\right\}$. Bob can deduce that Alice's secret information is 101 based on K_{AB}. Subsequently, Bob replaces the S_A sequence with the sequence $\left\{|1\rangle_{S_B}|1\rangle_{S_B}|0\rangle_{S_B}\right\}$ corresponding to his own secret message M_B, forming the sequence $\left\{|+\rangle_{D_B}|1\rangle_{S_B}|1\rangle_{D_B}|-\rangle_{D_B}|1\rangle_{S_B}|0\rangle_{S_B}\right\}$. Based on Alice's secret information $M_A=101$, Bob swaps the positions of $d_b^{1}=|+\rangle$ and $s_b^{1}=|1\rangle$, and $d_b^{3}=|-\rangle$ and $s_b^{3}=|0\rangle$, forming the sequence $S_B{}'=\left\{|1\rangle_{S_B}|+\rangle_{D_B}|1\rangle_{D_B}|0\rangle_{S_B}|1\rangle_{S_B}|-\rangle_{D_B}\right\}$ and sending it to Alice, where $\overline{S_B}=\left\{|1\rangle_{S_B}|0\rangle_{S_B}|1\rangle_{S_B}\right\}$, $\overline{D_B}=\left\{|+\rangle_{D_B}|1\rangle_{D_B}|-\rangle_{D_B}\right\}$. Alice can restore the sequences $\overline{S_B}$ and $\overline{D_B}$ to sequences S_B and D_B, she ultimately deduces Bob's secret information as 110.

Considering the inevitable influence of noise in actual quantum channels, the protocol can correct errors caused by noise by using error-correcting codes. In Step 1, by using the error-correcting code C_A, Alice can encode her secret information with C_A, and then she prepares $M_A\oplus C_A$ as the sequence of information particles S_A. The remaining steps remain unchanged. In Step 3 as well, Bob also uses error-correcting codes C_B to encode his secret message M_B. Ultimately, in this way, both communicating parties can correct errors and decode the original information sequences M_A and M_B.

The flowchart of the protocol is shown in Figure 3:

3 Security analysis

This section analyzes the potential security risks of the proposed SQD protocol, including intercept-resend attack, measure-resend attack, entangled-measure attack, and Trojan horse attack. It also considers the possibility of information leakage to ensure the

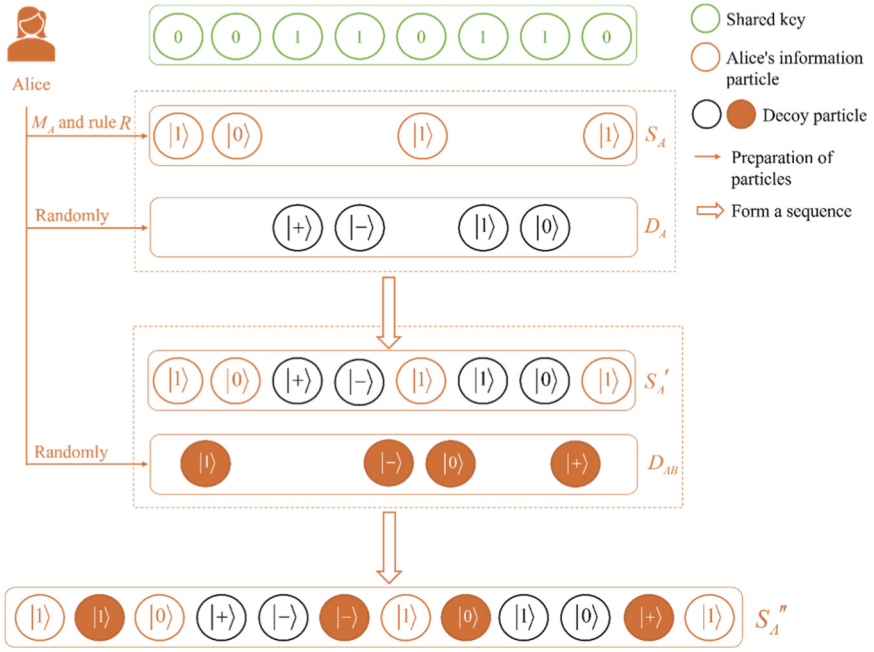

FIGURE 1
Alice's encoding process.

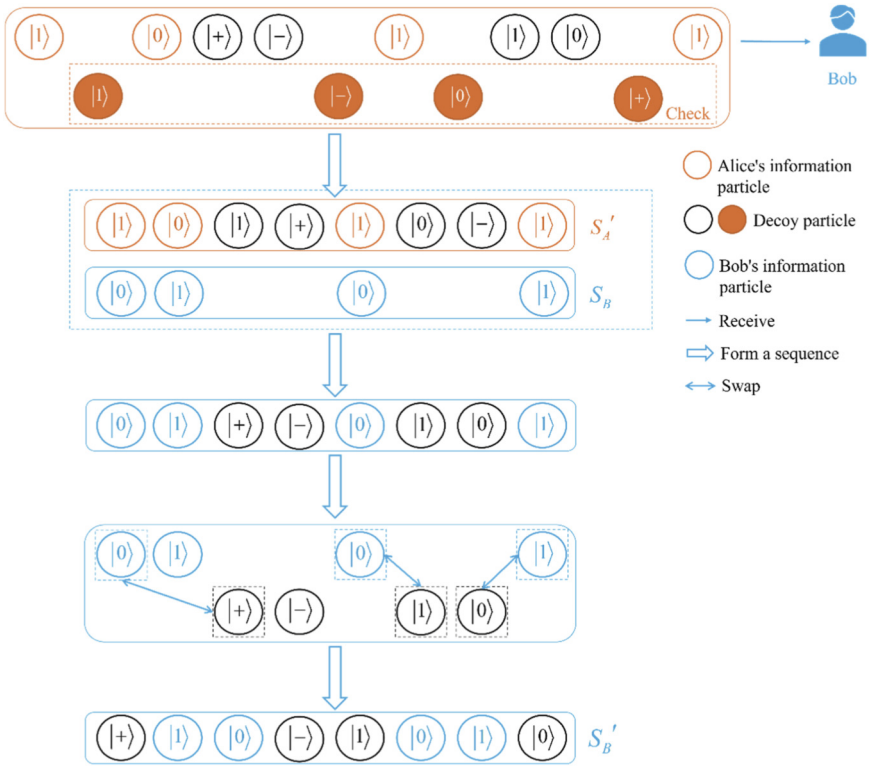

FIGURE 2
Bob's decryption and encryption operations.

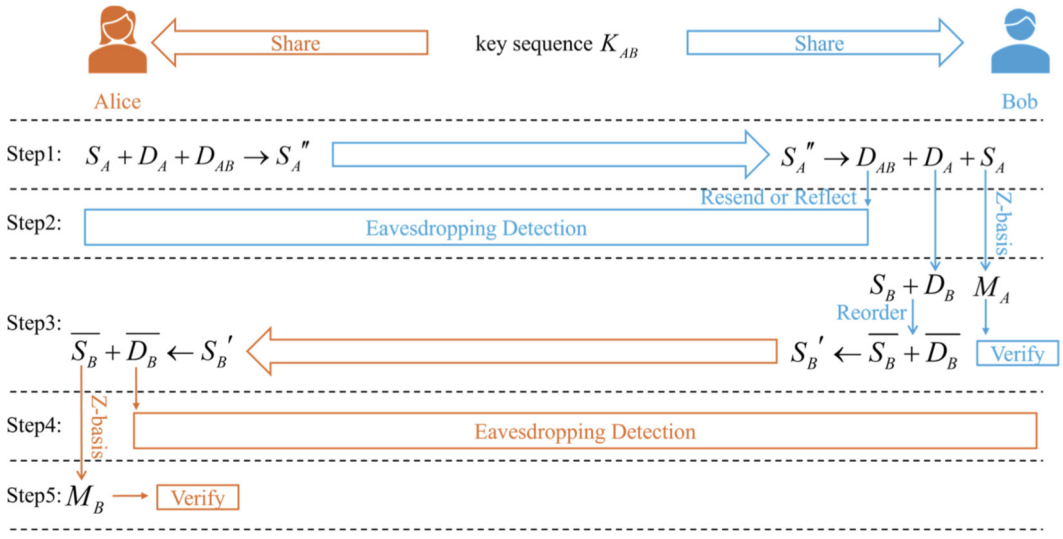

FIGURE 3
Flowchart of the proposed semi-quantum dialogue protocol.

protocol's overall security. Accordingly, the following evaluation will address these identified threats.

3.1 Intercept-resend attack

Eavesdropper Eve interferes with the communication between Alice and Bob by executing an intercept-resend attack. Eve may intercept and resend the sequence S_A'' transmitted from Alice to Bob in Step 2. Note that the sequence S_A'' contains both Alice's secret information sequence S_A, the decoy photon sequence D_A and decoy photon sequence D_{AB}. First, Eve lacks knowledge of the shared key K_{AB} between Alice and Bob, she cannot determine the positions of the particles belonging to the D_A and D_{AB} sequence. Second, Eve does not know the preparation basis of the decoy photons, Eve has a $\frac{1}{2}$ probability of resending in the Z-basis and a $\frac{1}{2}$ probability of resending in the X-basis $\{|+\rangle, |-\rangle\}$, At this point, two scenarios arise: if Bob chooses to measure, decoy photon is in the Z-basis, the probability that Eve passes the detection is $\frac{1}{2} \times \frac{1}{2} + \frac{1}{2} \times \frac{1}{2} = \frac{1}{2}$, if decoy photon is in the X-basis, Eve can pass the eavesdropping detection in this scenario; if Bob chooses to reflect, Eve has a $\frac{1}{2}$ probability of passing the eavesdropping detection. Eve has a $\frac{1}{2} \times \left(\frac{1}{2} \times \frac{1}{2} + \frac{1}{2} \times 1\right) + \frac{1}{2} \times \frac{1}{2} = \frac{5}{8}$ probability of passing the eavesdropping detection. However, when the number of decoy photons n is sufficiently large, the probability of Eve being detected is $1 - \left(\frac{5}{8}\right)^n$.

Similarly, Eve may intercept and resend the sequence S_B' transmitted from Bob to Alice in Step 4. It is observed that among the particles used for the second eavesdropping detection, approximately $\frac{1}{2}$ are in the Z-basis, while the remaining $\frac{1}{2}$ are in the X-basis. For the Z-basis, Eve's attack has a probability of $\frac{1}{2}$ to pass the detection; for the X-basis, Eve's attack has a probability of $\frac{1}{2}$ to pass the detection. Eve has a $\frac{1}{2} \times \frac{1}{2} + \frac{1}{2} \times \frac{1}{2} = \frac{1}{2}$ probability of passing the eavesdropping detection. Therefore, when the number of decoy particles n is sufficiently large, the probability that Eve is detected is $1 - \left(\frac{1}{2}\right)^n$.

It can be observed that Eve has a probability approaching 1 of being detected. In summary, the protocol we propose can effectively resist intercept-resend attacks.

3.2 Measure-resend attack

Eve attempts to obtain the secret information of Alice and Bob through a measure-resend attack. Specifically, Eve may intercept the sequence S_A'' sent to Bob by Alice in Step 2, and perform measurements on the particles, then resend the measured particles to Bob. However, since the sequence S_A'' is prepared by Alice based on the shared key K_{AB} with Bob, and Eve has no knowledge of the specific value of this key, even if she obtains the measurement results of S_A'', she cannot determine whether these results correspond to the secret information S_A or the decoy photons D_A and D_{AB}. Since decoy photons are randomly prepared in the Z-basis or X-basis, assume Eve's Z-basis measurement on the resent particles may yield outcomes corresponding to the Z-basis or the X-basis, At this point, two scenarios may occur: if Bob chooses to measure, the particle he measures must be the one resent by Eve. This action does not introduce an error rate; if Bob chooses to reflect, Eve measures a decoy photon with the Z-basis, the eavesdropping detection may pass. If Eve measures a decoy photon with the X-basis, there is a $\frac{1}{2}$ probability that her intervention will be detected during Alice's security check. For each decoy photon, Eve has a $\frac{1}{2} \times 1 + \frac{1}{2} \times \left(\frac{1}{2} \times 1 + \frac{1}{2} \times \frac{1}{2}\right) = \frac{7}{8}$ probability of passing the eavesdropping detection. However, the probability of Eve being detected is $1 - \left(\frac{7}{8}\right)^n$.

Similarly, Eve may measure and resend the sequence S_B' transmitted from Bob to Alice in Step 4. It is observed that among the particles used for the second eavesdropping detection, approximately $\frac{1}{2}$ are in the Z-basis, while the remaining $\frac{1}{2}$ are in

the X-basis. For the Z-basis, Eve's attack can pass the detection; for the X-basis, Eve's attack has a probability of $\frac{1}{2}$ to pass the detection. Eve has a $\frac{1}{2}\times 1+\frac{1}{2}\times\frac{1}{2}=\frac{3}{4}$ probability of passing the eavesdropping detection. Therefore, the probability that Eve is detected is $1-\left(\frac{3}{4}\right)^n$.

It can be concluded that when n is sufficiently large, Eve has a probability approaching 1 of being detected. Based on the above analysis, the protocol we propose can effectively resist measure-resend attack.

3.3 Entangled-measure attack

Eve attempts to obtain the secret information between Alice and Bob through an entanglement-measurement attack. Specifically, Eve may intercept the sequence S_A'' sent by Alice to Bob in Step 2 and perform a unitary operation U_E to entangle her own ancillary particles $|E\rangle$ with Alice's sequence S_A''. Eve's operation may transform the decoy photons into the following form:

$$U_E(|0\rangle|E\rangle)=\alpha|0\rangle|E_\alpha\rangle+\beta|1\rangle|E_\beta\rangle \tag{1}$$

$$U_E(|1\rangle|E\rangle)=\gamma|0\rangle|E_\gamma\rangle+\delta|1\rangle|E_\delta\rangle \tag{2}$$

$$\begin{aligned}U_E(|+\rangle|E\rangle)=\frac{1}{2}\big[&|+\rangle\left(\alpha|E_\alpha\rangle+\beta|E_\beta\rangle+\gamma|E_\gamma\rangle+\delta|E_\delta\rangle\right)\\&+|-\rangle\left(\alpha|E_\alpha\rangle-\beta|E_\beta\rangle+\gamma|E_\gamma\rangle-\delta|E_\delta\rangle\right)\big]\end{aligned} \tag{3}$$

$$\begin{aligned}U_E(|-\rangle|E\rangle)=\frac{1}{2}\big[&|+\rangle\left(\alpha|E_\alpha\rangle+\beta|E_\beta\rangle-\gamma|E_\gamma\rangle-\delta|E_\delta\rangle\right)\\&+|-\rangle\left(\alpha|E_\alpha\rangle-\beta|E_\beta\rangle-\gamma|E_\gamma\rangle+\delta|E_\delta\rangle\right)\big]\end{aligned} \tag{4}$$

In Equations 1–4, $|\alpha|^2+|\beta|^2=1$, $|\gamma|^2+|\delta|^2=1$ satisfying the normalization condition. $|E_\alpha\rangle$ and $|E_\beta\rangle$, $|E_\gamma\rangle$ and $|E_\delta\rangle$ represent the final states of Eve's ancillary particles after unitary evolution, and different quantum states are mutually orthogonal. Eve can obtain Alice's secret information by measuring her ancillary particle $|E\rangle$. It can be concluded that if Eve wishes to avoid detection of eavesdropping, she must ensure that $\beta=0$ and $\gamma=0$.However, under this condition, $\alpha|E_\alpha\rangle=\delta|E_\delta\rangle$, By comparing the expressions, it can be concluded that Eve cannot distinguish between the secret information states $|0\rangle$ and $|1\rangle$ through measurements on her ancillary particle $|E\rangle$. Therefore, if Eve attempts to steal the secret information of Alice and Bob via an entanglement-measurement attack without being detected, she cannot obtain any meaningful information.

Similarly, Eve may intercept the sequence S_B' sent by Bob to Alice in Step 4 and perform a unitary operation U_E to entangle her own ancillary particles $|E\rangle$ with Bob's sequence S_B'. Eve's entanglement operation may induce changes in all four types of decoy photons. If Eve attempts to extract information by measuring her auxiliary particles without being detected, she still cannot distinguish between states $|0\rangle$ and $|1\rangle$.

Based on the above analysis, the protocol we propose can effectively resist entanglement-measurement attacks.

3.4 Information leakage

The issue of classical correlation in quantum dialogue mentioned in [21, 22] refers to the potential leakage of approximately half of the secret information through classical channels. According to Shannon entropy theory [23], there are four possible combinations of secret information exchanged between Alice and Bob in each round of communication, each with a probability of $\frac{1}{4}$. The prior entropy is $H_{pri}=-\sum_{i=1}^{4}\frac{1}{4}\log_2\frac{1}{4}=2$. Since neither party discloses any content related to the secret information during the protocol, the posterior entropy remains $H_{pos}=-\sum_{i=1}^{4}\frac{1}{4}\log_2\frac{1}{4}=2$. The mutual information between the communicating parties (Alice and Bob) and Eve is $I(AB{:}E)=H_{pri}-H_{pos}=0$. Therefore, no information is leaked to Eve. Eve cannot attempt to obtain useful information by stealing the public information exchanged between Alice and Bob. In summary, the protocol we designed is resistant to information leakage.

3.5 Trojan horse attack

As noted in [24], Eve may utilize Trojan horse attacks to target the communication channel between Alice and Bob, primarily through delayed photon attack and invisible photon attack. A delayed photon attack involves Eve splitting a photon from a multi-photon pulse without altering the quantum state for eavesdropping purposes, while an invisible photon attack entails Eve injecting ancillary particles such as invisible wavelengths or delayed pulses into the communication devices to illicitly acquire information. To mitigate these threats, both communicating parties must implement filter to prevent unauthorized photon injections and photon beam separator to detect multi-photon anomalies. By integrating these countermeasures, our protocol effectively resists Trojan horse attacks.

3.6 The double CNOT attack

Eve attempts to obtain the secret information of Alice and Bob by using a double CNOT attack. Eve first prepares an auxiliary particle sequence S_E consisting of $3N$ particles initialized in the $|0\rangle$ state. She then intercepts the sequence S_A'' sent by Alice to Bob in Step 2 and performs a controlled-NOT (CNOT) operation, using sequence S_A'' as the control qubits and sequence S_E as the target qubits. Eve attempts to obtain Alice's secret message M_A by measuring her auxiliary particle sequence S_E^A. Afterward, Eve forwards the sequence S_A'' to Bob. Once Bob completes his encoding operation, Eve intercepts the encoded sequence S_B' again. She performs a second CNOT operation, taking sequence S_B' as the control qubits and sequence S_E^A as the target qubits. Finally, Eve attempts to extract Bob's secret message M_B by measuring the auxiliary particle sequence S_E^{AB}.

However, Eve's CNOT operations inevitably introduce noise and disturbances into the quantum channel, thereby altering the original quantum states. These disturbances will be detected during the first eavesdropping check. Furthermore, since Eve has no knowledge of the key value K_{AB}, she cannot correctly identify or distinguish the information particle sequences S_A corresponding to those particles. Consequently, Eve is unable to obtain Alice's secret message M_A. Moreover, Eve attempts to compare the measurement results of S_E^A and S_E^{AB} in an effort to identify the positions corresponding to the information particle sequence. However, after encoding, Bob rearranges the order of the information particles and decoy particles. Since Eve has no knowledge of M_A, she cannot

TABLE 2 Comparison with existing protocols.

Protocol	Type	Quantum channel	Measured basis	Public	Efficient
[26]	QD	Hyperentangled bell state	Bell, HBell	Yes	50%
[27]	QD	Two-particle product state	Z, X, bell	Yes	40%
[15]	SQD	Single photon	Z, X	Yes	66.7%
[16]	SQD	Bell state	Z, bell	Yes	20%
[18]	SQD	Hyperentangled bell state	Z, HBell	Yes	<15.4%
[19]	SQD	GHZ state	Z, GHZ	Yes	<16.7%
[20]	SQD	Four-particle Ω state	Z, Three-bit joint	Yes	55.6%
Our	SQD	Single photon	Z, X	No	100%

infer the rearrangement order. Consequently, she is unable to extract any useful information by comparing the measurement results of S_E^A and S_E^{AB}, and therefore cannot obtain Bob's secret message M_B.

After the above analysis, our protocol can effectively resist the double CNOT attack.

4 Efficiency analysis and comparison

The efficiency formula [25] for a quantum protocol is defined as: $\eta = \frac{b_s}{q_t+b_t}$, where b_s denotes the number of secret bits successfully exchanged between the parties, q_t represents the number of quantum qubits utilized (excluding those consumed for security checks), and b_t indicates the number of classical bits publicly communicated to facilitate the secret exchange. In the proposed protocol, the number of secret bits b_s mutually exchanged between Alice and Bob is $2N$. Alice uses N qubits to encode her secret information. After measuring Alice's secret information, Bob prepares N qubits carrying his own secret information to replace Alice's original N qubits. Thus, the total number of quantum bits is $q_t = 2N$. Since Alice and Bob do not disclose any information via a public channel that is relevant for mutual decryption, $b_t = 0$. The efficiency of this protocol is $\eta = \frac{2N}{2N} \times 100\% = 100\%$. We compared existing protocols with the proposed protocol, and the comparison results are summarized in Table 2. In the first row of the table, "Public" indicates whether the protocol discloses classical information for decryption purposes.

As summarized in Table 2, the proposed protocol exhibits clear advantages over existing full quantum dialogue protocols by substantially reducing the implementation burden on the semi-quantum party. Compared with representative semi-quantum protocols, our protocol requires a more easily realizable quantum channel, while the full-quantum party performs only single-qubit measurements, thereby lowering experimental complexity. In addition, no classical information related to decryption is disclosed during the protocol execution, which strengthens security and enhances overall communication efficiency. Consequently, the proposed protocol achieves superior efficiency relative to previously reported quantum dialogue protocols.

5 Conclusion

In summary, we propose an efficient semi-quantum dialogue protocol that employs single photons as quantum channels. During the initialization stage, the two communicating parties share a one-time random bit string, and then both parties securely encode and exchange messages through single photons. Finally, both parties can exchange their secret information securely. Security analysis shows that the protocol effectively resists common quantum attacks without information leakage. Moreover, compared with the existing SQD protocols, our protocol offers high security, improved efficiency, and better practical feasibility.

Data availability statement

The original contributions presented in the study are included in the article/supplementary material, further inquiries can be directed to the corresponding author.

Author contributions

J-TC: Writing – original draft. J-YL: Writing – original draft. X-JX: Writing – review and editing. C-YL: Writing – review and editing. F-GL: Writing – review and editing. LZ: Writing – review and editing.

Funding

The author(s) declared that financial support was received for this work and/or its publication. This research was supported by the National Natural Science Foundation of China (62272090), the Project of Science and Technology Tackling Key Problems in Henan Province (Grant nos 252102210178, 252102110182, 252102211105, 262102210208, and 262102210202), the Key Laboratory of Innovation and Testing Verification for Cryptographic Application Technology, Ministry of Industry and Information

Technology (Grant no. MMCXKT-2025-24), and Postgraduate Education Reform and Quality Improvement Project of Henan Province (YJS2025ZX10).

Conflict of interest

The author(s) declared that this work was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

Generative AI statement

The author(s) declared that generative AI was not used in the creation of this manuscript.

Any alternative text (alt text) provided alongside figures in this article has been generated by Frontiers with the support of artificial intelligence and reasonable efforts have been made to ensure accuracy, including review by the authors wherever possible. If you identify any issues, please contact us.

Publisher's note

All claims expressed in this article are solely those of the authors and do not necessarily represent those of their affiliated organizations, or those of the publisher, the editors and the reviewers. Any product that may be evaluated in this article, or claim that may be made by its manufacturer, is not guaranteed or endorsed by the publisher.

References

1. Bennett CH, Brassard G. Quantum cryptography: public key distribution and coin tossing. *Theor Computer Science* (2014) 560:7–11. doi:10.1016/j.tcs.2014.05.025

2. Hillery M, Bužek V, Berthiaume A. Quantum secret sharing. *Phys Rev A* (1999) 59:1829–34. doi:10.1103/physreva.59.1829

3. Karlsson A, Koashi M, Imoto N. Quantum entanglement for secret sharing and secret splitting. *Phys Rev A* (1999) 59:162–8. doi:10.1103/physreva.59.162

4. Xiao L, Lu Long G, Deng FG, Pan JW. Efficient multiparty quantum-secret-sharing schemes. *Phys Rev A—Atomic, Mol Opt Phys* (2004) 69:052307. doi:10.1103/physreva.69.052307

5. Cabello A. Quantum key distribution without alternative measurements. *Phys Rev A* (2000) 61:052312. doi:10.1103/physreva.61.052312

6. Deng FG, Long GL, Liu XS. Two-step quantum direct communication protocol using the einstein-podolsky-rosen pair block. *Phys Rev A* (2003) 68:042317. doi:10.1103/physreva.68.042317

7. Deng FG, Long GL. Secure direct communication with a quantum one-time pad. *Phys Rev A—Atomic, Mol Opt Phys* (2004) 69:052319. doi:10.1103/physreva.69.052319

8. Nguyen BA. Quantum dialogue. *Phys Lett A* (2004) 328:6–10. doi:10.1016/j.physleta.2004.06.009

9. Zhong-Xiao M, Zhan-Jun Z, Yong L. Quantum dialogue revisited. *Chin Phys Lett* (2005) 22:22–4. doi:10.1088/0256-307x/22/1/007

10. Yang CW, Hwang T. Quantum dialogue protocols immune to collective noise. *Quan Information Processing* (2013) 12:2131–42. doi:10.1007/s11128-012-0514-4

11. Dai J, Zhang S, Chang Y, Li X, Zheng T, Xia J. A controlled quantum dialogue protocol based on quantum walks. *Comput Mater and Continua* (2020) 64:905–19. doi:10.32604/cmc.2020.010550

12. Maitra A. Measurement device-independent quantum dialogue. *Quan Inf Process* (2017) 16:305. doi:10.1007/s11128-017-1757-x

13. Boyer M, Kenigsberg D, Mor T. Quantum key distribution with classical bob. In: *Proceedings of the 2007 first international conference on quantum, nano, and micro technologies (ICQNM'07)*. New York, NJ, USA: IEEE (2007). p. 10. Guadeloupe, Franch, 2–6 January 2007.

14. Shukla C, Thapliyal K, Pathak A. Semi-quantum communication: protocols for key agreement, controlled secure direct communication and dialogue. *Quan Inf Process* (2017) 16:295. doi:10.1007/s11128-017-1736-2

15. Ye TY, Ye CQ. Semi-quantum dialogue based on single photons. *Int J Theor Phys* (2018) 57:1440–54. doi:10.1007/s10773-018-3672-z

16. Pan HM. Semi-quantum dialogue with bell entangled states. *Int J Theor Phys* (2020) 59:1364–71. doi:10.1007/s10773-019-04335-w

17. Shi GF. Cryptanalysis and improvement of semi-quantum dialogue with bell entangled states. *Int J Theor Phys* (2023) 62:224. doi:10.1007/s10773-023-05482-x

18. Shi GF. Semi-quantum dialogue scheme based on hyperentangled bell states. *Physica Scripta* (2023) 98:115120. doi:10.1088/1402-4896/ad007f

19. Yang CW, Liu PY. Semi-quantum dialogue based on GHZ states. *Quan Inf Process* (2025) 24:1–18. doi:10.1007/s11128-025-04833-3

20. Li ZZ, He RZ, Zhang ZZ, Ding HY, Wang DF. Semi-quantum dialogue protocol based on four-particle Ω state. *Chin J Phys* (2025) 95:348–57. doi:10.1016/j.cjph.2025.03.003

21. Tan YG, Cai QY. Classical correlation in quantum dialogue. *Int J Quan Inf* (2008) 6:325–9. doi:10.1142/s021974990800344x

22. Gao F, Guo F, Wen Q, Zhu F. Revisiting the security of quantum dialogue and bidirectional quantum secure direct communication. *Sci China Ser G: Phys Mech Astron* (2008) 51:559–66. doi:10.1007/s11433-008-0065-y

23. Shannon CE. Communication theory of secrecy systems. *Bell System Technical Journal* (1949) 28:656–715. doi:10.1002/j.1538-7305.1949.tb00928.x

24. Cai Q. Eavesdropping on the "ping-pong" type quantum communication protocols with invisible photon. *Phys Lett A* (2006) 351:23–5. doi:10.1016/j.physleta.2005.10.050

25. Cabello A. Quantum key distribution in the holevo limit. *Phys Rev Lett* (2000) 85:5635–8. doi:10.1103/PhysRevLett.85.5635

26. Han KQ, Zhou L, Zhong W, Sheng YB. Measurement-device-independent quantum dialogue based on hyperentanglement. *Quan Inf Process* (2021) 20:280. doi:10.1007/s11128-021-03213-x

27. Pan TJ, Zhou RG, Zhang XX. Three-party quantum dialogue based on Grover's algorithm with identity dual authentication. *Quan Inf Process* (2024) 23:365. doi:10.1007/s11128-024-04570-z