entropy

IMPACT FACTOR 2.0

Indexed in: PubMed

CITESCORE 5.2

Article

Improvement of Three-Party Semi-Quantum Protocol for Deterministic Secure Quantum Dialogue Based on GHZ States

Ling Zhang, Xun Liu, Xiang-Jun Xin, Chao-Yang Li and Li Gong

MDPI

https://doi.org/10.3390/e27101002

entropy

MDPI

Article

Improvement of Three-Party Semi-Quantum Protocol for Deterministic Secure Quantum Dialogue Based on GHZ States

Ling Zhang, Xun Liu *, Xiang-Jun Xin, Chao-Yang Li and Li Gong

College of Software Engineering, Zhengzhou University of Light Industry, Zhengzhou 450002, China; ll790217@163.com (L.Z.)
* Correspondence: 332316020972@zzuli.edu.cn

Abstract

Through the analysis of "Three-party semi-quantum protocol for deterministic secure quantum dialogue based on GHZ states", we demonstrate that the protocol is vulnerable to attacks from dishonest participants. Specifically, the fully quantum-capable participant may behave dishonestly, leading the two semi-quantum participants to receive incorrect secret information, with the dishonest behavior remaining undetected. Accordingly, we propose an improved protocol that demonstrates robustness against various internal and external attacks, including dishonest participant attacks, and we further prove that it does not suffer from information leakage. Moreover, compared to the original protocol, the improved version achieves a significant enhancement in quantum communication efficiency.

Keywords: semi-quantum dialogue; GHZ state; dishonest participant attack

1. Introduction

The quantum dialogue protocol is a secure communication protocol based on the principles of quantum communication. In 2004, Nguyen et al. [1] first introduced the concept of Quantum Dialogue (QD) protocols. By utilizing Bell states as the quantum channel, their protocol enabled two communicating parties to exchange secret messages simultaneously and securely, leveraging the entanglement property of Bell states. Shortly thereafter, in 2005, Man et al. [2] identified a critical vulnerability in Nguyen's protocol [1], demonstrating that it could not resist intercept–resend attacks, and proposed an improved version to enhance its security. As research progressed, a variety of QD protocols were developed using different types of quantum states as communication channels, such as GHZ states [3,4] and single photons [5,6], thereby enriching the diversity and applicability of protocol designs. However, in 2008, Gao et al. [7] revealed that several existing protocols [2,3,5] suffer from information leakage, where an adversary can infer partial secret information based on the classical messages disclosed during the communication process. This finding brought significant attention to the problem of information leakage, which has since become a key consideration in the design of secure QD protocols [8–10].

Beyond conventional two-party communication, efforts were made to broaden the scope of QD protocols. In 2007, Xia et al. [11] proposed the Controlled Quantum Dialogue (CQD) protocol, introducing a third-party controller who supervises the dialogue between two legitimate communicators without directly participating in the transmission of secret information. Since then, CQD has become an important research branch in the field of QD, leading to a series of protocols with improved efficiency, security, and practical feasibility [12–14]. However, it is worth noting that although a third-party controller is

check for updates

Academic Editor: Rosario Lo Franco

Received: 23 August 2025
Revised: 22 September 2025
Accepted: 24 September 2025
Published: 26 September 2025

Citation: Zhang, L.; Liu, X.; Xin, X.-J.; Li, C.-Y.; Gong, L. Improvement of Three-Party Semi-Quantum Protocol for Deterministic Secure Quantum Dialogue Based on GHZ States. *Entropy* **2025**, *27*, 1002. https://doi.org/10.3390/e27101002

introduced in some protocols, such as CQD, the aforementioned schemes remain fundamentally two-party in nature, as the controller does not engage in the exchange of secret messages. As a result, these protocols are not applicable to scenarios where all three participants wish to exchange secret information with one another. Fortunately, as research has progressed, quantum dialogue protocols have expanded beyond the limitation of only two participants. Many quantum dialogue protocols that allow for multi-party participation have been successfully designed. In these multi-party quantum dialogue protocols, all participants can share their information and obtain the secret information of the other participants. In 2016, Yu et al. [15] proposed a three-party quantum dialogue protocol based on continuous-variable GHZ states, which can be further extended to accommodate a larger number of communicating participants. In 2017, Cao et al. [16] introduced a multi-party quantum dialogue protocol based on multi-particle GHZ states. This protocol can be implemented using optical devices with high transmission efficiency, making it highly practical. Subsequently, in 2018, Gong et al. [17] proposed another multi-party quantum dialogue protocol based on continuous-variable GHZ states, which can also be more easily realized using controllable optical devices and has the potential to significantly enhance the channel capacity.

All of the above quantum dialogue protocols always require both participants to possess quantum capabilities. However, not every participant can afford expensive quantum devices. In 2007, Boyer et al. [18] proposed the first semi-quantum secret protocol, in which only one of the two participants possesses quantum capabilities, while the other one requires only classical abilities. Specifically, we distinguish between fully quantum participants, who can perform all quantum operations (including preparation, transmission, storage, and measurement in arbitrary bases), and semi-quantum participants, whose capabilities are restricted to simple operations such as preparing or measuring qubits in the computational basis, reflecting qubits without disturbance, and reordering them. This novel concept has since been applied to various quantum cryptography tasks, such as quantum key distribution (QKD) [19,20], quantum secure direct communication (QSDC) [21,22], and quantum secret sharing (QSS) [23,24]. In 2017, Shukla et al. [25] proposed the first semi-quantum dialogue protocol. Since then, a growing number of semi-quantum dialogue protocols have been developed to effectively reduce the reliance on quantum resources. Recent advancements include standard semi-quantum dialogue protocols [10,26,27] and multi-party semi-quantum dialogue protocols [28,29]. In the context of multi-party semi-quantum dialogue, Xu et al. [28] proposed the first three-party protocol based on cluster states in 2020, wherein two participants with only semi-quantum capabilities can successfully complete the dialogue, and the protocol exhibits relatively high efficiency.

Recently, a three-party semi-quantum dialogue quantum based on GHZ states was proposed by Zhou et al. [29] (Hereafter, we call this three-party SQD protocol the ZZL-SQD). This protocol allows each participant to share their secret and obtain the secrets of the other two participants, with one participant having full quantum capabilities and the other two participants having only semi-quantum abilities. Moreover, Zhou et al. have verified that the protocol can effectively resist various attacks, including intercept–measure attack, flip attack, man-in-the-middle attack, and entangle–measure attack; at the same time, it also demonstrates a high qubit efficiency. However, we will demonstrate that when the ZZL-SQD protocol is attacked by a dishonest participant, the two semi-quantum participants in the protocol will receive the wrong secret information about each other and will not detect the attack. Furthermore, we propose effective improvements to the ZZL-SQD protocol to defend against the aforementioned insider attack, while also enhancing its qubit efficiency. The main contributions of this work are summarized as follows:

(1) We identify a critical security flaw in the original ZZL-SQD protocol—specifically, its inability to defend against attacks launched by dishonest participants—and provide a detailed analysis accompanied by concrete examples to illustrate this vulnerability.
(2) To address potential attacks from dishonest participants, we propose an improved version of the ZZL-SQD protocol and conduct a comprehensive security analysis, demonstrating that the revised scheme is robust against various external and internal attacks and effectively prevents information leakage.
(3) We further evaluate the quantum communication efficiency of the proposed protocol. The results demonstrate a notable improvement over the original ZZL-SQD protocol, thereby enhancing its overall practicality and applicability.

The rest of this paper is arranged as follows: Section 2 gives a brief description of the ZZL-SQD protocol. Section 3 introduces the security analysis of ZZL-SQD protocol against dishonesty and presents an improvement. Section 4 analyzes its security and Section 5 provides the comparison. Finally, Section 6 makes a conclusion.

2. Description of the ZZL-SQD Protocol

Firstly, we briefly review the ZZL-SQD protocol. Suppose there are three participants: Alice, Bob, and Charlie. Each of them aims to share their information and obtain the secret information of the other participants. Alice, as the quantum participant, possesses complete quantum resources, while Bob and Charlie are semi-quantum participants with limited capabilities. The protocol consists of the following steps.

$$\left|\Psi_{q_1,q_2,q_3}\right\rangle_{ABC} = \frac{1}{\sqrt{2}}\left(|q_1,q_2,q_3\rangle + (-1)^{\Delta}|\overline{q_1,q_2,q_3}\rangle\right)_{ABC} \tag{1}$$

Initialization: Alice, Bob, and Charlie each have n bits of secret information, denoted as m_A, m_B and m_C, respectively.

Step 1: Alice randomly prepares n GHZ states according to Equation (1) and obtains a sequence of GHZ states, denoted as S, where $q_1 = 0$, $q_2, q_3 \in \{0,1\}$ and $\Delta \in \{0,1\}$. She then partitions each GHZ state into three particles: S_A, S_B, and S_C. Next, Alice randomly prepares $4n$ decoy photons using measurement bases X or Z. She inserts $2n$ decoy photons into sequences S_B and S_C, resulting in two new particle sequences, $\overline{S}_B$ and $\overline{S}_C$. Alice keeps S_A and sends $\overline{S}_B$ and $\overline{S}_C$ to Bob and Charlie, respectively.

Step 2: After Bob and Charlie receive the sequence, respectively, Alice announces the positions of all the decoy photons in $\overline{S}_B$ and $\overline{S}_C$. Bob and Charlie use quantum delay line to temporarily store sequences and then select the first n decoy photons from the $2n$ ones, which they received to conduct the first eavesdropping check. They randomly perform one of the following two operations on the decoy photons:

(1) M: Measure the decoy photon using the Z-basis and prepare a photon in the same state as the measurement result, then send it back to Alice.
(2) R: Directly reflect the photon to Alice without making any disturbance.

Step 3: Once Alice confirms that she has received all the returned decoy photons, Bob and Charlie announce the positions of the corresponding n decoy photons, the operations performed, and the measurement results, respectively. Alice then performs the first eavesdropping check. For the photons on which the M operation was performed, Alice measures the received decoy photons using the Z-basis, compares the measurement results with those announced by Bob and Charlie, and calculates the error rate. For the photons on which the R operation was performed, Alice measures them using the basis she originally used when preparing the corresponding photons and calculates the error rate. If

the overall error rate exceeds a predefined threshold, the protocol is terminated and the communication is aborted; otherwise, the protocol continues.

Step 4: Bob and Charlie each separate the remaining n decoy photons from $\overline{S}_B$ and $\overline{S}_C$, then obtain sequences S_B and S_C, respectively. Then, Bob (Charlie) performs Z-basis measurements on the particles in $S_B(S_C)$ and records the measurement results. Next, Bob (Charlie) encrypts the information particle sequence according to their secret information $m_B(m_C)$ using the following encryption rule:

(1) If $m_B^i(m_C^i)$ is 1, Bob (Charlie) prepares a state in the Z-basis that is the opposite of the measurement result of the corresponding particle $S_B^i(S_C^i)$.
(2) If $m_B^i(m_C^i)$ is 0, Bob (Charlie) does nothing.

After Bob (Charlie) completes the encryption process, the sequence $S_B(S_C)$ is transformed into $S'_B(S'_C)$. For the remaining n decoy photons, Bob (Charlie) randomly performs one of the following two operations:

(1) MM: Measure the decoy photon using the Z-basis and prepare a photon in the same state as the measurement result.
(2) RR: Do nothing; Once all decoy photons have been processed, Bob (Charlie) reorders all the particles in the sequence $S'_B(S'_C)$ to obtain a new sequence $S''_B(S''_C)$. Bob and Charlie then send S''_B and S''_C to Alice, respectively.

Step 5: Similar to step 3, Alice performs the second eavesdropping detection on sequences S''_B and S''_C, finally calculates the error rate and determines whether to terminate the protocol.

Step 6: After the second eavesdropping check is passed, Bob and Charlie announce the correct order of the information particles in the sequences S''_B and S''_C to Alice. This allows Alice to recover the sequences S'_B and S'_C after removing the decoy photons. Alice performs measurements on the particle sequences S_A, S'_B, and S'_C in the Z-basis, obtaining the corresponding measurement result sequences R_A, R'_B and R'_C. Ultimately, Alice can deduce Bob's and Charlie's secret information. Alice then announces the values of $R_A \oplus R'_B \oplus R'_C$ and $m_A \oplus R_A$, and reveals the initial GHZ states based on the positions of each particle in the sequences S_B and S_C. Consequently, Bob or Charlie can infer the secret information of the other two participants based on the information published by Alice.

3. Analysis and Improvement of ZZL-SQD Protocol

3.1. Security Analysis of ZZL-SQD Protocol Against the Dishonest Participant Attack

Zhou et al. proved that their protocol can resist various attacks, such as flip attacks, intercept–measure attacks, man-in-the-middle attacks, and entangle–measure attacks. The analysis showed that the protocol can both avoid information leakage problems and detect a variety of attacks employed by external adversaries like Eve. However, they did not consider the possibility of an internal dishonest participant attack, in which one participant in the protocol may have dishonest behavior to cause other participants to receive incorrect secret information, and such dishonest behavior would not be detected.

For the ZZL-SQD protocol, Alice could potentially become a dishonest participant, and she can keep Bob and Charlie from getting the correct secret information about each other by announcing false classic information.

Here, we provide an example. Suppose the initial GHZ state prepared by Alice is $|\Psi_{000}\rangle_{ABC} = \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)_{ABC}$, and the secret information of Alice, Bob, and Charlie is 0, 1, and 1, respectively. Bob and Charlie will measure the received information particles and then prepare states opposite to the measurement results, which are then inserted into the sequences S'_B and S'_C. Assume the initial GHZ state $|\Psi_{000}\rangle_{ABC}$ collapses into the state $|000\rangle_{ABC}$ after Bob and Charlie's measurements. After completing the second

eavesdropping check, Alice performs Z-basis measurements on her particles, and the information particles encoded by Bob and Charlie, the resulting state will be $|011\rangle_{ABC}$. From this, Alice can infer that both Bob's and Charlie's secret information is 1 by performing an XOR operation, as shown in Equations (2) and (3).

$$m_B^i = R_B^i \oplus R_B^{i\prime} = 0 \oplus 1 = 1 \tag{2}$$

$$m_C^i = R_C^i \oplus R_C^{i\prime} = 0 \oplus 1 = 1 \tag{3}$$

Then Alice announces the initial GHZ state is $|\Psi_{000}\rangle_{ABC}$, as well as the values of $R_A^i \oplus R_B^{i\prime} \oplus R_C^{i\prime}$ and $m_A^i \oplus R_A^i$, as shown in Equations (4) and (5).

$$R_A^i \oplus R_B^{i\prime} \oplus R_C^{i\prime} = 0 \oplus 1 \oplus 1 = 0 \tag{4}$$

$$m_A^i \oplus R_A^i = 0 \oplus 0 = 0 \tag{5}$$

For Bob, after performing Z-basis measurements on his information particles, he obtains the result $R_B^i = 0$. Therefore, he can deduce that the entangled state $|\Psi_{000}\rangle_{ABC}$ collapsed to $|000\rangle_{ABC}$, and subsequently determine $R_A^i = 0$ and $R_C^i = 0$. Bob can then calculate Charlie's secret information based on the value of $m_A^i \oplus R_A^i$, R_A^i, and R_C^i, as shown in Equation (6).

$$m_C^i = R_C^{i\prime} \oplus R_C^{\mathrm{i}} = \left(R_A^i \oplus R_B^{i\prime} \oplus R_C^{i\prime}\right) \oplus R_A^i \oplus R_B^{\mathrm{i}\prime} \oplus R_C^{\mathrm{i}} = 0 \oplus 0 \oplus 1 \oplus 0 = 1 \tag{6}$$

Bob can also calculate Alice's secret information based on the values of $m_A^i \oplus R_A^i$ and R_A^i, as shown in Equation (7).

$$m_A^i = \left(m_A^i \oplus R_A^i\right) \oplus R_A^i = 0 \oplus 0 = 0 \tag{7}$$

Charlie obtains Bob's and Alice's secret information using a process similar to the one described above, so the details are not repeated here.

However, if Alice is dishonest and publishes 1 as the value of $R_A^i \oplus R_B^{i\prime} \oplus R_C^{i\prime}$, which is the opposite of the value of Equation (4), the corresponding Bob can deduce that Charlie's secret value is 0, as shown in Equation (8).

$$m_C^i = R_C^{i\prime} \oplus R_C^{\mathrm{i}} = \left(R_A^i \oplus R_B^{i\prime} \oplus R_C^{i\prime}\right) \oplus R_A^i \oplus R_B^{\mathrm{i}\prime} \oplus R_C^{\mathrm{i}} = 1 \oplus 0 \oplus 1 \oplus 0 = 0 \tag{8}$$

Charlie deduces that the value of Bob's secret is 0, as shown in Equation (9).

$$m_B^i = R_B^{i\prime} \oplus R_B^{\mathrm{i}} = \left(R_A^i \oplus R_B^{i\prime} \oplus R_C^{i\prime}\right) \oplus R_A^i \oplus R_C^{\mathrm{i}\prime} \oplus R_B^{\mathrm{i}} = 1 \oplus 0 \oplus 1 \oplus 0 = 0 \tag{9}$$

Ultimately, Bob and Charlie get the wrong secret information about each other because of Alice's operation. They didn't know that Alice had published false information, because Alice had more responsibility and authority than Bob and Charlie, yet Bob and Charlie couldn't be sure that Alice was acting honestly. Specifically, Bob and Charlie just perform different operations on the received particles and then return them to Alice, who is responsible for performing the two rounds of eavesdropping checks and announcing the classical information. After completing the second eavesdropping check, Alice can deduce Bob's and Charlie's secret information first, then publish the valid classic information and let Bob and Charlie calculate the secret information. However, to obtain the secret information about Alice and Charlie (Bob), Bob (Charlie) must rely entirely on the classical information announced by Alice, but he cannot verify the correctness of the classical information published by Alice and the secret information calculated by himself. This allows Alice to

modify the public classical information, making it easy for Bob and Charlie to obtain the tampered secret information, and the attack can be successfully executed without being detected by Bob and Charlie.

3.2. Improvement of ZZL-SQD Protocol

In the ZZL-SQD protocol, Alice is assumed to be a trusted participant. However, considering the crucial need to enhance security against the potential dishonesty of any participant in semi-quantum communication protocols [30,31], we propose an improved protocol that eliminates the requirement for a trusted Alice. The schematic diagram of the improved ZZL-SQD protocol is shown in Figure 1. Before the protocol begins, all participants use a one-way hash function $H : \{0,1\}^* \to \{0,1\}^n$. The content of the improved protocol is as follows:

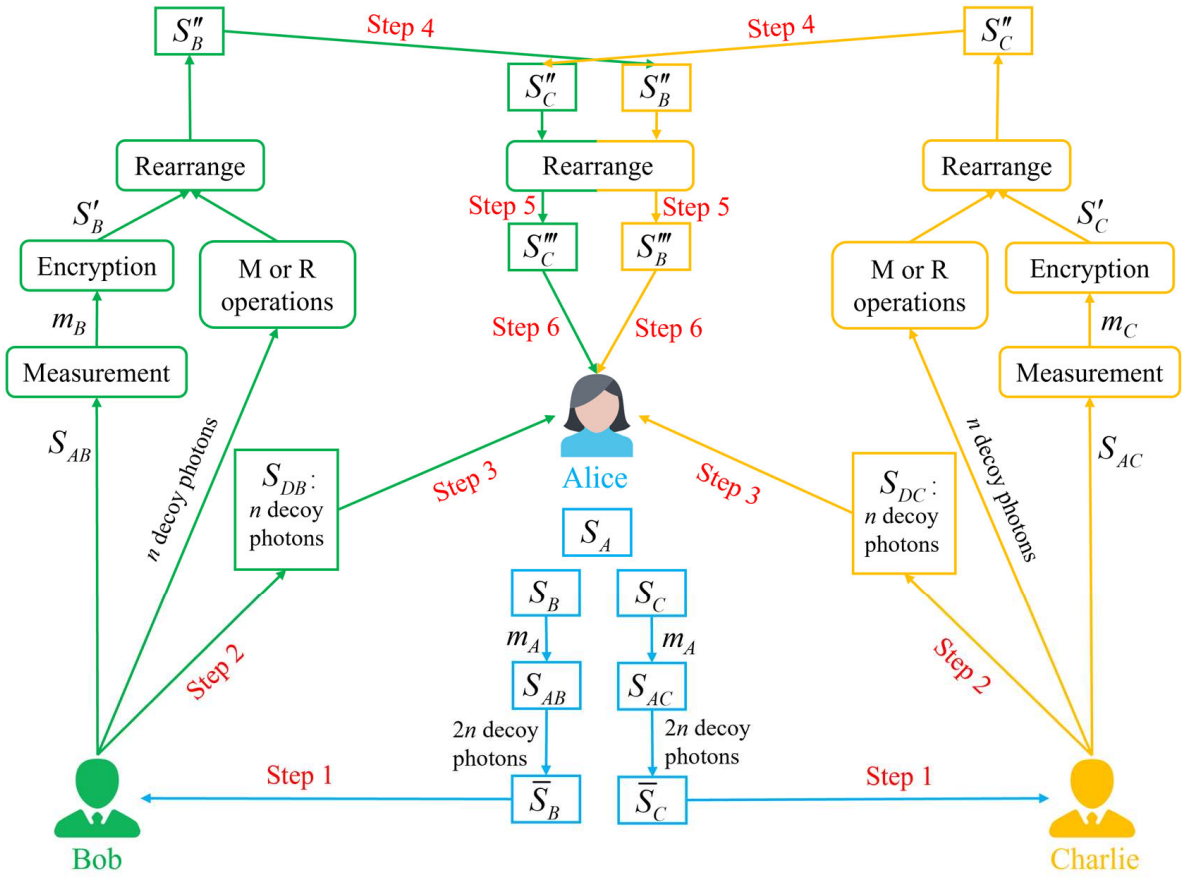

Figure 1. The schematic diagram of the improved ZZL-SQD protocol.

Step1: Alice randomly prepares n GHZ states according to Equation (1) and obtains a sequence of GHZ states, denoted as S, where $q_1 = 0$, $q_2, q_3 \in \{0,1\}$ and $\Delta \in \{0,1\}$, and where the value of n is a public parameter known to all participants. She then partitions the particles according to their positions into three separate information particle sequences: S_A, S_B, and S_C, corresponding to the first, second, and third particles of each GHZ state, respectively. Next, Alice performs encryption operations on the particle sequences S_B and S_C based on the n-long binary secret information m_A, resulting in the new sequence S_{AB} and S_{AC}, respectively. The encryption rule is defined as follows: if $m_A^i = 0 (i \in n)$, no operation is applied to the corresponding particles S_B^i and S_C^i; if $m_A^i = 1 (i \in n)$, a Pauli-X operation (δ_X) is applied to both particles S_B^i and S_C^i. The Pauli-X operation flips the state of a qubit, e.g., $\delta_X|0\rangle = |1\rangle, \delta_X|1\rangle = |0\rangle$. She then randomly generates $4n$ decoy photons in either the X- or Z-basis, and inserts $2n$ of them into the sequences S_{AB} and S_{AC}, respectively,

resulting in the modified sequences $\overline{S}_B$ and $\overline{S}_C$. Finally, Alice keeps S_A and sends $\overline{S}_B$ and $\overline{S}_C$ to Bob and Charlie, respectively.

Step 2: Upon Bob (Charlie) receiving each particle from the sequence $\overline{S}_B(\overline{S}_C)$, Alice announces whether the particle at the corresponding position is a decoy photon. For the first n decoy photons in $\overline{S}_B(\overline{S}_C)$, Bob and Charlie randomly choose to perform one of the following two operations:(1) M: Measure the decoy photon in the Z-basis and prepare a new photon in the corresponding measured state; (2) R: Perform no operation. By employing quantum delay lines, Bob (Charlie) then applies a reordering operation to these n decoy states to form the sequence $S_{DB}(S_{DC})$. Finally, Bob and Charlie respectively send S_{DB} and S_{DC} to Alice.

Step 3: This step is identical to Step 3 of the original ZZL-SQD protocol.

Step 4: Based on the information announced by Alice, Bob (Charlie) can distinguish the information particles from the remaining n decoy photons in the sequence $\overline{S}_B(\overline{S}_C)$. For the information particles, Bob (Charlie) performs Z-basis measurements on the information particles in $S_{AB}(S_{AC})$ and records the measurement results. Next, Bob (Charlie) encrypts the information particle sequence according to their secret information $m_B(m_C)$ using the following encryption rule: (1): If $m_B^i(m_C^i)$ is 1, Bob (Charlie) prepares a state in the Z-basis that is the opposite of the measurement result of the corresponding particle $S_B^i(S_C^i)$. (2): If $m_B^i(m_C^i)$ is 0, Bob (Charlie) does nothing. After Bob (Charlie) completes the encryption process, the sequence $S_{AB}(S_{AC})$ is transformed into $S'_B(S'_C)$. For the remaining n decoy photons, Bob and Charlie randomly perform either the R or M operation as described in Step 2. By employing quantum delay lines, Bob (Charlie) reorders all decoy photons and the particles in the sequence $S'_B(S'_C)$ to obtain sequence $S''_B(S''_C)$. Eventually, Bob and Charlie send S''_B and S''_C to each other.

Step 5: Upon Charlie receiving each particle from the sequence S''_B, Bob announces whether the particle at the corresponding position is an information particle. Charlie only performs Z-basis measurements on the information particles in S''_B and records the corresponding results. Ultimately, Charlie rearranges all the information particles and decoy photons to obtain the new sequence S'''_B. Similarly, upon Bob receiving each particle from the sequence S''_C, Charlie announces whether the particle at the corresponding position is an information particle. Bob only performs Z-basis measurements on the information particles in S''_C and records the corresponding results. Ultimately, Bob rearranges all the information particles and decoy photons to obtain the new sequence S'''_C. Bob and Charlie then send S'''_B and S'''_C to Alice, respectively.

Step 6: After confirming Alice has received S'''_B and S'''_C, Bob and Charlie announce the positions, operations and measurement results of the corresponding n decoy photons in the sequences, respectively. Similar to step 3, Alice performs the same operation on these decoy photons as the first eavesdropping detection, then she calculates the error rate and determines whether to terminate the protocol.

Step 7: After the second eavesdropping check is passed, Bob and Charlie announce the correct order of the information particles in S'''_B and S'''_C to Alice. This allows Alice to recover the sequences S'_B and S'_C after removing the decoy photons. Then, Alice performs Z-basis measurements on the particles in sequences S_A, S'_B, and S'_C, obtaining the corresponding measurement result sequences R_A, R'_B and R'_C. Alice announces the values of $H(R'_B)$ and $H(R'_C)$, which are verified by Bob and Charlie for correctness. If both are correct, Alice can deduce the correct secret information of Bob and Charlie. Alice then announces the values of R_A and reveals the initial GHZ states based on the positions of each particle in the sequences S_B and S_C. Consequently, Bob or Charlie can infer the secret information of the other two participants based on the information published by Alice.

4. Security Analysis

The quantum dialogue protocol enables communication between participants over a quantum channel. However, during this process, potential adversaries may launch various attacks to intercept the transmission of secret information. These adversaries are typically categorized into two types: external adversaries and internal adversaries (dishonest participants). Internal adversaries were first introduced by Gao et al. in 2007 [32]. Gao et al. emphasized that dishonest participants possess greater capabilities than external attackers, making them more likely to either steal secret information from other participants or manipulate the accuracy of the information received by others, all without detection. Moreover, in contrast to the original protocol, our improved version introduces an additional step wherein Bob and Charlie exchange particle sequences via a dedicated quantum channel. This modification, however, introduces potential vulnerabilities to previously negligible or irrelevant attacks—including, but not limited to, intercept–resend, measurement–resend, and Trojan horse attacks specifically targeting the Bob-Charlie link. In this section, we conduct a security analysis of the improved protocol, focusing on two critical aspects: external attack and dishonest participant attack. Additionally, an analysis of potential information leakage is also essential to ensure the protocol's robustness.

4.1. External Attack

An external attacker (commonly denoted as Eve) is assumed to possess full quantum capabilities. By eavesdropping on the quantum channel, Eve may launch various types of attacks, including the intercept–prepare–resend attack, intercept–measure-resend attack, entangle–measurement attack, and Trojan horse attack, in an attempt to eavesdrop on or interfere with the communication process.

4.1.1. Intercept–Prepare–Resend Attack

In an intercept–prepare–resend attack, the external eavesdropper Eve first prepares a set of fake single-particle states in either the X-basis or the Z-basis. She then performs eavesdropping by intercepting the quantum channel between any two participants. For each qubit in the quantum sequence transmitted from the sender to the receiver, Eve discards the original particle and replaces it with one of her own fake particles, which is then forwarded to the intended recipient. Since Eve does not perform any measurement on the intercepted particles, she avoids directly disturbing the entangled state's collapse. However, in the proposed improved protocol, such an attack inevitably introduces detectable errors. The core reason lies in the protocol's use of decoy photons randomly prepared in the four quantum states $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$. Bob and Charlie randomly perform either R or M operation on these decoy photons, each with equal probability of $1/2$. Taking Bob as an example: When Bob performs the R operation, Eve has a $1/4$ probability of having prepared a state that is identical to the original decoy photon, which would not introduce any error. She also has a $1/4$ chance of preparing the orthogonal state, which will certainly result in a detectable error when Alice performs her measurement. Additionally, with a $1/2$ probability, Eve prepares a non-orthogonal state (e.g., the original decoy photon is $|+\rangle$, but the fake state is $|0\rangle$ or $|1\rangle$), which introduces an error with a probability of $1/2$ upon Alice's measurement. When Bob performs the M operation, similar statistical outcomes apply. Eve has a $1/4$ chance of correctly guessing and preparing the same state as Bob's resending, introducing no error. She also has a $1/4$ probability of preparing the orthogonal state, which causes a definite error. In the remaining $1/2$ of cases, Eve prepares a non-orthogonal state (e.g., Bob resends $|0\rangle$, but Eve replaces it with $|+\rangle$ or $|-\rangle$), which leads to an error with a probability of $1/2$ during Alice's measurement.

In summary, for the n decoy photon used in each eavesdropping detection process, the probability that Eve will be detected by launching an intercept–prepare–resend attack is $1-\left(2\times\frac{1}{2}\times\left(\frac{1}{4}\times 1+\frac{1}{2}\times\frac{1}{2}\right)\right)^{n}=1-\left(\frac{1}{2}\right)^{n}$.

4.1.2. Intercept–Measure–Resend Attack

In an intercept–measure-resend attack, Eve performs eavesdropping on the quantum channel between any two participants. For each particle in the quantum sequence transmitted from the sender to the receiver, Eve intercepts the particle and measures it in either the Z-basis or the X-basis. She then prepares a new particle in the measured state and sends it to the intended recipient. However, under the proposed improved protocol, such an attack inevitably introduces detectable errors due to the presence of decoy photons. Specifically, decoy photons are randomly prepared in one of the four states $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$, and Bob and Charlie randomly choose to perform either R or a M operation on each received photon, with equal probability. Taking Bob as an example: If Bob performs the R operation, Eve has a $1/2$ chance of selecting the same basis as Alice's preparation basis. In this case, the measured state remains consistent with the original, and no error is introduced. However, with the remaining $1/2$ probability, Eve measures the particle in the opposite basis (e.g., the decoy photon is prepared in $|+\rangle$, but Eve uses the Z-basis). In such cases, there is a $1/2$ chance that Alice's final measurement will detect an inconsistency, thereby revealing Eve's presence; If Bob performs the M operation, the decoy photon will eventually collapse into one of the computational basis states, $|0\rangle$ or $|1\rangle$, and Bob resends the result to Alice. If Eve uses the Z-basis to measure the photon, her action does not alter the outcome and no error is introduced. Conversely, if she uses the X-basis for measurement, there will be a $1/2$ probability that the state she resends leads to an error when Alice performs her measurement.

In summary, for the n decoy photon used in each eavesdropping detection process, the probability that Eve will be detected by launching an intercept–measure-resend attack is $1-\left(2\times\frac{1}{2}\times\left(\frac{1}{2}\times 1+\frac{1}{2}\times\frac{1}{2}\right)\right)^{n}=1-\left(\frac{3}{4}\right)^{n}$.

4.1.3. Entangle–Measurement Attack

In an entangle–measurement attack, the eavesdropper Eve does not directly measure or tamper with the particles transmitted through the quantum channel. Instead, she applies a unitary operation U_E that entangles each transmitted particle with an auxiliary particle $|E\rangle$ of her own. This strategy enables Eve to delay her measurement and optimize it later based on the classical information publicly announced during the protocol, thereby increasing her chance of extracting useful secret information. However, in the proposed improved protocol, Eve is unaware of the exact positions of the decoy photons. To maximize the effectiveness of her attack, she must apply the entangling operation U_E indiscriminately to all transmitted particles, including both decoy and information particles. Suppose the transmitted qubit is in the state $|0\rangle$ or $|1\rangle$; the unitary operation U_E acts as follows:

$$\begin{aligned} U_E(|0\rangle|E\rangle) &= \alpha_0|0\rangle|E_{00}\rangle+\beta_0|1\rangle|E_{01}\rangle \\ U_E(|1\rangle|E\rangle) &= \alpha_1|0\rangle|E_{10}\rangle+\beta_1|1\rangle|E_{11}\rangle \end{aligned} \tag{10}$$

The parameters α_0 and β_0, as well as α_1 and β_1, satisfy $|\alpha_0|^2+|\beta_0|^2=1$ and $|\alpha_1|^2+|\beta_1|^2=1$, respectively. To avoid introducing errors during eavesdropping detection,

Eve must ensure that the entangled quantum state remains unchanged, which requires $\beta_0 = \alpha_1 = 0$. Thus, we obtain Equation (11):

$$\begin{aligned} U_E(|0\rangle|E\rangle) &= \alpha_0|0\rangle|E_{00}\rangle \\ U_E(|1\rangle|E\rangle) &= \beta_1|1\rangle|E_{11}\rangle \end{aligned} \tag{11}$$

When the transmitted particle is $|+\rangle$ or $|-\rangle$, it follows from Equation (11) that the unitary operation U_E acts on these states as:

$$\begin{aligned} U_E(|+\rangle|E\rangle) &= U_E\left(\tfrac{|0\rangle+|1\rangle}{\sqrt{2}}|E\rangle\right) = \tfrac{1}{\sqrt{2}}(\alpha_0|0\rangle|E_{00}\rangle + \beta_1|1\rangle|E_{11}\rangle) \\ &= \tfrac{1}{2}[(\alpha_0|E_{00}\rangle + \beta_1|E_{11}\rangle)|+\rangle + (\alpha_0|E_{00}\rangle - \beta_1|E_{11}\rangle)|-\rangle] \\ U_E(|1\rangle|E\rangle) &= U_E\left(\tfrac{|0\rangle-|1\rangle}{\sqrt{2}}|E\rangle\right) = \tfrac{1}{\sqrt{2}}(\alpha_0|0\rangle|E_{00}\rangle - \beta_1|1\rangle|E_{11}\rangle) \\ &= \tfrac{1}{2}[(\alpha_0|E_{00}\rangle - \beta_1|E_{11}\rangle)|+\rangle + (\alpha_0|E_{00}\rangle + \beta_1|E_{11}\rangle)|-\rangle] \end{aligned} \tag{12}$$

Clearly, if Eve intends to avoid introducing errors during the subsequent eavesdropping detection, her entangling operation must ensure that the quantum state of the transmitted particle remains unchanged. This requirement leads to the condition expressed in Equation (13).

$$\alpha_0|E_{00}\rangle = \beta_1|E_{11}\rangle \tag{13}$$

Based on Equations (11)–(13), it can be concluded that if Eve's attack is to remain undetectable, the measurement outcomes on her auxiliary particles must be statistically independent of the quantum states transmitted between the legitimate participants. This implies that Eve cannot extract any meaningful information about the secret messages from her entangled ancillary system. Therefore, the proposed improved SQD protocol is secure against entangle measurement attack.

4.1.4. Trojan Horse Attack

On the quantum channel between Alice and Bob, and between Alice and Charlie, Eve eavesdrops by launching two common Trojan Horse attacks, invisible photon attacks [33], and delayed photon attacks [34]. Nevertheless, Alice, Bob, and Charlie can detect these attacks using filter and photon number splitter techniques before measuring or reflecting on the particles they receive.

4.2. Dishonest Participant Attack

In the original ZZL-SQD protocol, Alice, as a potentially dishonest participant, may attempt to interfere with the dialogue between Bob and Charlie by manipulating the quantum communication process. In contrast, under the improved protocol proposed in this study, if Alice intends to achieve the same objective, her dishonest behavior would have to occur in one of the following two scenarios: (1) launching an attack on the quantum channel during Step 4, when Bob and Charlie exchange their encrypted sequences; (2) publishing false classical information during Step 7 in an attempt to mislead the recovery of secret messages. The following provides a rigorous analysis of both scenarios, demonstrating that under the improved protocol, Alice's dishonest intentions cannot be successfully realized.

For the first case, consider the transmission of the quantum sequence S_B'' from Bob to Charlie. If Alice intends to compromise Charlie's recovery of Bob's secret information, she must first extract the encrypted content from S_B'' and then alter the corresponding quantum states. However, in Step 4, the sequence S_B'' is generated by Bob through randomly rearranging a mixture of decoy photons and information particles. The exact positions of the information qubits are disclosed only after Charlie has acknowledged receipt of each individual particle. As analyzed in Section 4.1, if Alice attempts to interfere without

knowing the rearrangement order—by launching intercept–prepare–resend, intercept–measure-resend, entangle–measurement attacks—such interference will disturb the decoy states with non-zero probability, which in turn affects the protocol's ability to detect attacks launched by potential external adversaries. This would compromise the subsequent eavesdropping detection and increase the likelihood of being discovered. Since Alice also serves as both a participant and a verifier in the eavesdropping check, any tampering she performs would undermine the protocol's ability to ensure secure transmission and thereby increase the risk of secret information being compromised. Consequently, such attacks are self-defeating and cannot be used to disrupt the communication between Bob and Charlie.

In the second case, Alice is required to publish classical information in Step 7, which enables Bob and Charlie to infer the collapsed states of the information particles in the sequences S_B and S_C. Based on this, each of them combines the classical data with their measurement outcomes on the encrypted sequences S_{AB} and S_{AC}, respectively, to reconstruct Alice's secret message m_A. If Alice dishonestly publishes incorrect measurement results, the immediate consequence is a disruption in her own communication with Bob and Charlie, rather than in the dialogue between Bob and Charlie themselves. This result contradicts her intention as a dishonest participant, which is to interfere with others' communication while maintaining her own message intact.

It is noteworthy that Bob and Charlie, as participants, may also exhibit dishonest behavior. They could potentially launch attacks against particles traversing the quantum channel or perform dishonest operations on the received particles. However, on the one hand, due to their limited semi-quantum capabilities, any attempt to interfere with particles in the quantum channel—as analyzed in Section 4.1 regarding external attacks—would not afford them any advantage over a fully quantum-equipped Eve in evading detection. On the other hand, taking Bob as an example, he might perform Z-basis measurements on the information particles from sequence S'_C received in Step 5 and subsequently prepare counterfeit states opposite to his measurement outcomes instead of forwarding the original particles. Nevertheless, in Step 7, Alice measures the sequence S'_C to obtain R'_C and publicly announces the value of $H(R'_C)$. Since Charlie also has knowledge of R'_C, she can verify whether the particles in S'_C were altered by Bob's operations by computing and comparing the resulting values. Any inconsistency would reveal Bob's dishonest activity. Similarly, if Charlie were to engage in analogous particle counterfeiting, her dishonest behavior could be detected by Alice and Bob in Step 7.

In summary, the protocol demonstrates strong robustness and security against internal attacks launched by dishonest participants.

4.3. Information Leakage

In a quantum dialogue protocol, if an external eavesdropper Eve can deduce part or all of the secret information solely based on the classical information publicly announced by legitimate participants—without launching any active attack—then the protocol is considered to suffer from a potential information leakage risk. In our proposed improved protocol, such a risk may only theoretically arise in Step 6, where Alice discloses the value of R_A along with the corresponding initial GHZ states for each particle in the sequences S_B and S_C. This information allows Eve to infer the collapsed states of all initial GHZ states under Z-basis measurement, denoted as S_A, S_B and S_C. However, before being sent to Bob and Charlie, the S_B and S_C sequences are encrypted using Alice's secret message m_a, resulting in the ciphertext sequences S_{AB} and S_{AC}, respectively. Without performing any active attack, Eve has no access to the states of these sequences. Therefore, the only way she can attempt to retrieve Alice's secret is through random guessing. For each bit of Alice's message, Eve has a probability of $1/2$ to guess correctly. According to information

theory, this corresponds to an entropy of $-\sum_{i=1}^{n} P_i \log_2 P_i = -\left(2 \times \frac{1}{2} \times \left(\log_2 \frac{1}{2}\right)\right) = 1$ bit per secret bit, indicating that the classical information published by Alice does not reveal her secret.

Furthermore, Bob's and Charlie's messages are also encrypted within the S_{AB} and S_{AC} sequences, which are protected by a second round of eavesdropping detection. Without knowledge of the pre-encryption and post-encryption states, Eve can also only rely on random guessing to infer Bob's and Charlie's secrets. The guessing probability and information entropy for each bit remain the same, i.e., 1 bit, indicating that the classical information published by Alice does not reveal Bob and Charlie's secrets.

In summary, there will be no information leakage problem in the improved protocol.

5. Efficiency Analysis

Qubit efficiency is one of the key indicators for evaluating the practicality of a quantum communication protocol. It can be formally calculated using the efficiency formula proposed by Cabello [35]: $\eta = \frac{b_s}{q_s+q_t}$ where b_s denotes the total number of secret bits successfully transmitted, and q_s and q_t represent the total number of qubits and classical bits consumed for transmitting these secret messages, respectively. Note that decoy photons and classical bits used solely for eavesdropping detection are excluded from this calculation. Table 1 summarizes a comparative analysis of our proposed protocol with several existing three-party QD protocols.

Table 1. The comparison with some existing three-party QD protocols.

	[15]	[16]	[28]	ZZL-SQD Protocol	This Work
Protocol Type	Fully Quantum	Fully Quantum	Semi-Quantum	Semi-Quantum	Semi-Quantum
Communication Pattern	Symmetric	Asymmetric	Asymmetric	Symmetric	Symmetric
Quantum Resources	Continuous variable GHZ states	4-dimensional 4-particle entangled GHZ states	Four-particle cluster states	GHZ states	GHZ states
Analysis dishonest participant attack	No	Yes	Yes	No	Yes
b_s	$6n$	$6n$	$4n$	$6n$	$6n$
q_t	$3n$	$8n$	$8n$	$3n$	$3n$
q_s	$9n$	0	$2n$	$5n$	$4n$
η	66.7%	75%	20%	75%	85.7%

In protocol [15], all three participants possess full quantum capabilities and follow a symmetric communication model, where each participant is able to both send and receive n bits of secret information to and from the other two participants. This results in a total of $6n$ secret bits exchanged. Alice prepares a sequence of n continuous-variable GHZ states to carry the secret messages, consuming $3n$ qubits. For classical communication, each participant announces their measurement results twice for a sequence of n particles, yielding a total of $3n$ classical bits. Thus, the overall quantum bit efficiency of protocol [15] is $\eta = \frac{6n}{3n+6n} \approx 0.667$.

In protocol [16], the system includes a semi-honest third party (TP) and three fully quantum-capable participants, who engage in symmetric communication. Each participant is able to send and receive n bits of secret information to and from the other two, resulting in $6n$ secret bits exchanged. TP prepares a sequence of n four-dimensional four-particle entangled GHZ states to carry the secret messages, resulting in a consumption

of $q_s = \log_2 4 \times 4 \times n = 8n$ qubits. No classical bits are used for transmitting the secret messages. Therefore, the total quantum bit efficiency of protocol [16] is $\eta = \frac{6n}{8n} = 0.75$.

In protocol [28], the communication scenario involves one fully quantum participant, Charlie, and two semi-quantum participants, Alice and Bob. The communication pattern is asymmetric, as it enables bidirectional message exchange only between Charlie and Alice (or Bob), while direct communication between Alice and Bob is not supported. In this protocol, both Alice and Bob transmit n bits of secret information to Charlie, and Charlie likewise sends n bits to each of them, yielding a total of $4n$ secret bits transmitted. To enable this, Charlie prepares $2n$ four-particle cluster states, corresponding to $8n$ qubits used. Additionally, Charlie discloses $2n$ classical bits to publish his encoding sequences. As a result, the overall qubit efficiency of this protocol is $\eta = \frac{4n}{8n+2n} = 0.2$.

In contrast, the original ZZL-SQD protocol adopts a symmetric communication model, where each participant is able to both send and receive n bits of secret information to and from the other two participants. This yields a total of 6n secret bits exchanged. Alice prepares a sequence of n GHZ states to carry the secret messages, resulting in $3n$ qubits. For classical communication, Alice publishes $3n$ bits to reveal the initial GHZ states, n bits for Bob's and Charlie's secret message sequence, and another n bits for her own message sequence, summing up to $5n$ bits. Thus, the total efficiency of the ZZL-SQD protocol is $\eta = \frac{6n}{3n+5n} = 0.75$.

Our improved protocol also adopts a symmetric communication structure, maintaining full two-way information exchange between all three participants. Each of them receives n bits of secret messages from the other two, again yielding a total of $6n$ bits. Alice prepares n GHZ states for message transmission, requiring $3n$ qubits. The classical communication involves the publication of $3n$ bits to indicate the initial GHZ states and n bits for the measurement results of particle sequence S_A, giving a total of $4n$ bits. Consequently, the qubit efficiency of the improved protocol reaches $\eta = \frac{6n}{3n+4n} \approx 0.857$.

These results demonstrate that, in addition to providing enhanced resistance against insider attacks, our improved protocol also achieves a significant increase in quantum communication efficiency compared to both the original ZZL-SQD protocol and other protocol, thereby offering greater practicality and scalability in real-world quantum communication scenarios.

6. Conclusions

In summary, this work first provides a brief overview of the original ZZL-SQD protocol and presents a rigorous analysis demonstrating its vulnerability to attacks from dishonest participants. To address this issue, we propose an effective improvement scheme. The improved ZZL-SQD protocol ensures symmetric communication among participants without requiring any enhancement of their quantum capabilities. From a security standpoint, the protocol addresses the original scheme's inability to resist dishonest participant attack, and further demonstrates robustness against various external and internal attack scenarios, while effectively preventing information leakage. In addition, the improved protocol achieves a notable enhancement in quantum communication efficiency, making it significantly more practical and feasible for real-world applications compared to the original protocol.

Author Contributions: L.Z. and X.L. wrote the main manuscript text; X.-J.X. and C.-Y.L. gave the modified advice to improve the manuscript; L.G. prepared Table 1. All authors have read and agreed to the published version of the manuscript.

Funding: 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), and Postgraduate Education Reform and Quality Improvement Project of Henan Province (YJS2025ZX10).

Institutional Review Board Statement: Not applicable.

Data Availability Statement: Not applicable.

Conflicts of Interest: The authors declare no conflicts of interest.

References

1. Nguyen, B.A. Quantum dialogue. *Phys. Lett. A* **2004**, *328*, 6–10. [CrossRef]
2. Man, Z.X.; Zhang, Z.J.; Li, Y. Quantum dialogue revisited. *Chin. Phys. Lett.* **2005**, *22*, 22. [CrossRef]
3. Man, Z.X.; Xia, Y.J. Controlled Bidirectional Quantum Direct Communication by Using a GHZ State. *Chin. Phys. Lett.* **2006**, *23*, 1680. [CrossRef]
4. Xia, Y.; Fu, C.B.; Zhang, S.; Hong, S.K.; Yeon, K.H.; Um, C.I. Quantum dialogue by using the GHZ state. *arXiv* **2006**, arXiv:quant-ph/0601127.
5. Ji, X.; Zhang, S. Secure quantum dialogue based on single-photon. *Chin. Phys. B* **2006**, *15*, 1418–1420.
6. Yang, Y.; Wen, Q. Quasi-secure quantum dialogue using single photons. *Sci. China Phys. Mech. Astron.* **2007**, *50*, 558–562. [CrossRef]
7. Gao, F.; Guo, F.; Wen, Q.; Zhu, F. Revisiting the security of quantum dialogue and bidirectional quantum secure direct communication. *Sci. China Phys. Mech. Astron.* **2008**, *51*, 559–566. [CrossRef]
8. Gao, G. Two quantum dialogue protocols without information leakage. *Opt. Commun.* **2010**, *283*, 2288–2293. [CrossRef]
9. Lang, Y.-F.; Cai, C.-C. Quantum dialogue with one qubit to represent two bits. *Quantum Inf. Process.* **2024**, *23*, 396. [CrossRef]
10. Li, Z.Z.; He, R.Z.; Zhang, Z.Z.; Ding, H.Y.; Wang, D.F. Semi-quantum dialogue protocol based on four-particle Ω state. *Chin. J. Phys.* **2025**, *95*, 348–357. [CrossRef]
11. Yan, X.; Jie, S.; Jing, N.; He-Shan, S. Controlled Secure Quantum Dialogue Using a Pure Entangled GHZ States. *Commun. Theor. Phys.* **2007**, *48*, 841. [CrossRef]
12. Ai, Z.; Yin, A. Controlled and authenticated quantum dialogue protocol based on Grover's algorithm. *Int. J. Theor. Phys.* **2022**, *61*, 261. [CrossRef]
13. Liu, B.-X.; Liang, X.-Q. Novel controlled quantum dialogue protocols without information leakage. *Int. J. Theor. Phys.* **2022**, *61*, 51. [CrossRef]
14. Wang, C.; Zhu, H. An Authenticated Controlled Quantum Dialogue Protocol Using Double-Linked GHZ-Like States in Cross-domain Setting. *Int. J. Theor. Phys.* **2023**, *62*, 211. [CrossRef]
15. Yu, Z.-B.; Gong, L.-H.; Zhu, Q.-B.; Cheng, S.; Zhou, N.-R. Efficient three-party quantum dialogue protocol based on the continuous variable GHZ states. *Int. J. Theor. Phys.* **2016**, *55*, 3147–3155. [CrossRef]
16. Cao, G.; Jiang, M. Multi-party quantum dialogue protocol based on multi-particle GHZ states. In Proceedings of the 2017 Chinese Automation Congress (CAC), Jinan, China, 20–22 October 2017; IEEE: New York, NJ, USA, 2017; pp. 1614–1618.
17. Gong, L.; Tian, C.; Li, J.; Zou, X. Quantum network dialogue protocol based on continuous-variable GHZ states. *Quantum Inf. Process.* **2018**, *17*, 331. [CrossRef]
18. 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), Guadeloupe, Franch, 2–6 January 2007; IEEE: New York, NJ, USA, 2007; p. 10.
19. Dong, S.; Mi, S.; Hou, Q.; Huang, Y.; Wang, J.; Yu, Y.; Wei, Z.; Zhang, Z.; Fang, J. Decoy state semi-quantum key distribution. *EPJ Quantum Technol.* **2023**, *10*, 18. [CrossRef]
20. Ye, C.-Q.; Li, J.; Chen, X.-B.; Hou, Y.; Wang, Z. Security and application of semi-quantum key distribution protocol for users with different quantum capabilities. *EPJ Quantum Technol.* **2023**, *10*, 21. [CrossRef]
21. Tian, Y.; Zhang, N.; Chang, J.; Li, J. Three-party semi-quantum secure direct communication based on two communication models. *Phys. Scr.* **2024**, *99*, 095110. [CrossRef]
22. Zhang, X.-X.; Zhou, R.-G.; Xu, W.-S. Robust semi-quantum secure direct communication based on multi-particle system. *Quantum Inf. Process.* **2025**, *24*, 169. [CrossRef]
23. He, F.; Xin, X.; Li, C.; Li, F. Security analysis of the semi-quantum secret-sharing protocol of specific bits and its improvement. *Quantum Inf. Process.* **2024**, *23*, 51. [CrossRef]
24. Xin, X.; He, F.; Li, C.; Li, F. Multiparty semi-quantum secret sharing protocol based on single photon sequence and permutation. *Mod. Phys. Lett. A* **2024**, *39*, 2450084. [CrossRef]
25. Shukla, C.; Thapliyal, K.; Pathak, A. Semi-quantum communication: Protocols for key agreement, controlled secure direct communication and dialogue. *Quantum Inf. Process.* **2017**, *16*, 295. [CrossRef]

26. Pan, H.-M. Semi-quantum dialogue with Bell entangled states. *Int. J. Theor. Phys.* **2020**, *59*, 1364–1371. [CrossRef]
27. Zhang, L.; Liu, X.; Xin, X.-J.; Li, P.; Li, C.-Y. Semi-Quantum Dialogue with d-Dimensional Single Particles. *Int. J. Theor. Phys.* **2025**, *64*, 133. [CrossRef]
28. Xu, L.-C.; Chen, H.-Y.; Zhou, N.-R.; Gong, L.-H. Multi-party semi-quantum secure direct communication protocol with cluster states. *Int. J. Theor. Phys.* **2020**, *59*, 2175–2186. [CrossRef]
29. Zhou, R.-G.; Zhang, X.; Li, F. Three-party semi-quantum protocol for deterministic secure quantum dialogue based on GHZ states. *Quantum Inf. Process.* **2021**, *20*, 153. [CrossRef]
30. Liu, L.; Xiao, M.; Song, X. Authenticated semiquantum dialogue with secure delegated quantum computation over a collective noise channel. *Quantum Inf. Process.* **2018**, *17*, 342. [CrossRef]
31. Zhao, M.-N.; Zhou, R.-G.; Feng, Y.-H. Multi-Party Controlled Semi-Quantum Dialogue Protocol Based on Hyperentangled Bell States. *Entropy* **2025**, *27*, 666. [CrossRef] [PubMed]
32. Gao, F.; Qin, S.J.; Wen, Q.Y.; Zhu, F.C. A simple participant attack on the brádler-dušek protocol. *Quantum Inf. Comput.* **2007**, *7*, 329–334. [CrossRef]
33. Cai, Q.-Y. Eavesdropping on the two-way quantum communication protocols with invisible photons. *Phys. Lett. A* **2006**, *351*, 23–25. [CrossRef]
34. Gisin, N.; Ribordy, G.; Tittel, W.; Zbinden, H. Quantum cryptography. *Rev. Mod. Phys.* **2002**, *74*, 145. [CrossRef]
35. Cabello, A. Quantum key distribution in the Holevo Limit. *Phys. Rev. Lett.* **2000**, *85*, 5635. [CrossRef]