entropy

IMPACT FACTOR 2.0

Indexed in: PubMed

CITESCORE 5.2

Article

Multi-Party Controlled Semi-Quantum Dialogue Protocol Based on Hyperentangled Bell States

Meng-Na Zhao, Ri-Gui Zhou and Yun-Hao Feng

MDPI

https://doi.org/10.3390/e27070666

entropy

MDPI

Article

Multi-Party Controlled Semi-Quantum Dialogue Protocol Based on Hyperentangled Bell States

Meng-Na Zhao, Ri-Gui Zhou * and Yun-Hao Feng

School of Information Engineering, Shanghai Maritime University, Shanghai 201306, China; z783809615@163.com (M.-N.Z.); email_yhfeng@163.com (Y.-H.F.)
* Correspondence: rgzhou@shmtu.edu.cn

Abstract

To solve the fundamental problem of excessive consumption of classical resources and the simultaneous security vulnerabilities in semi-quantum dialogue systems, a multi-party controlled semi-quantum dialogue protocol based on hyperentangled Bell states is proposed. A single controlling party is vulnerable to information compromise due to tampering or betrayal; the multi-party controlled mechanism ($Charlie_1$ to $Charlie_n$) in this protocol establishes a distributed trust model. It mandates collective authorization from all controlling parties, significantly enhancing its robust resilience against untrustworthy controllers or collusion attacks. The classical participant Bob uses an adaptive Huffman compression algorithm to provide a framework for information transmission. This encoding mechanism assigns values to each character by constructing a Huffman tree, generating optimal prefix codes that significantly optimize the storage space complexity for the classical participant. By integrating the "immediate measurement and transmission" mechanism into the multi-party controlled semi-quantum dialogue protocol and coupling it with Huffman compression coding technology, this framework enables classical parties to execute encoding and decoding operations. The security of this protocol is rigorously proven through information-theoretic analysis and shows that it is resistant to common attacks. Furthermore, even in the presence of malicious controlling parties, this protocol robustly safeguards secret information against theft. The efficiency analysis shows that the proposed protocol provides benefits such as high communication efficiency and lower resource consumption for classical participants.

Keywords: hyperentangled bell states; Huffman compression coding; multi-party controlled; semi-quantum dialogue

Received: 3 June 2025
Revised: 19 June 2025
Accepted: 20 June 2025
Published: 21 June 2025

Citation: 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. https://doi.org/10.3390/e27070666

1. Introduction

Quantum secure direct communication (QSDC) is a significant branch within the quantum cryptography framework, achieving the transmission of ciphertext directly through a quantum channel without the need for pre-shared keys [1]. In 2003, Deng et al. pioneered the two-step QSDC protocol based on EPR entangled pairs [2], establishing the core criteria of QSDC for the first time: qubits serve as both information carriers and eavesdropping detection, alongside the necessity of a post-selection mechanism for information decoding. To address vulnerabilities associated with measurement devices, the Zhou team [3] proposed the first measurement-device-independent (MDI) QSDC protocol in 2020. In the same year, Wu et al. [4] innovatively utilized hyperentangled states of photon polarization-spatial mode dual degrees of freedom (DOF) to construct a high-capacity

MDI-QSDC protocol. In recent years, researchers have made milestone progress in experimental studies of QSDC [5,6]. Particularly noteworthy is Qi et al.'s proposal in 2021 [7] of a QSDC network based on time-energy entanglement and sum-frequency generation, which established a secure quantum entanglement channel over 40 km of fiber by implementing quantum memory functionality through adjustments to circuit delay modules. By 2023, Wang et al. [8] realized the first real-time QSDC network based on computationally secure relays, providing reliable experimental evidence for further research and advancing QSDC towards practical application stages.

Quantum dialogue (QD), as a bidirectional extension paradigm of QSDC, facilitates interactive information exchange between two parties over a quantum channel. The QD protocol framework was first introduced by Nguyen [9] in 2004, which addressed the limitations of one-way communication in QSDC. However, Gao et al. [10] revealed in their 2008 study that QD protocols commonly suffer from information leakage vulnerabilities. This finding spurred research into anti-leakage mechanisms as a core topic. In 2014, the Ye team [11] innovatively introduced EPR pairs as private quantum keys, using dynamic unitary rotations to encrypt transmitted photons in real time, successfully overcoming the issue of information leakage in QD. In 2015, Yin et al. [12] utilized a class of three-qubit W-states and quantum dense coding techniques to achieve a QD protocol with zero information leakage. In 2018, Qi et al. [13] proposed the first controlled quantum dialogue (CQD) protocol with an authentication mechanism, which successfully defended against both internal and external attacks. In 2021, Han et al. [14] presented an MDI-QD protocol based on hyperentanglement, which effectively eliminated security vulnerabilities and information leakage issues related to measurement devices. In 2023, Lin et al. [15] proposed two efficient fault-tolerant QD protocols tailored for collective noise channels, designing and implementing quantum logic circuits for practical demonstration. Zhu et al. [16] proposed a one-step QD protocol based on hyperentanglement, which greatly simplified experimental procedures and reduced message loss due to photon transmission losses. Wang et al. [17] extended QD to quantum communication networks using cluster states, eliminating the need for trusted node assumptions and achieving higher fidelity in transmission. Additionally, in 2025, Lang et al. [18] proposed a rapid quantum dialogue protocol that operates without unitary operations or auxiliary photons. Also in the same year, Huang et al. [19] introduced a counterfactual controlled QD protocol based on entanglement swapping, demonstrating that neither physical transmission of particles nor prior entanglement between remote participants is required, significantly enhancing system security.

The engineering deployment of quantum communication systems faces core bottlenecks in the high cost and low accessibility of quantum devices. To address these challenges, Boyer et al. first proposed the Semi-Quantum Key Distribution (SQKD) protocol in 2009 [20], successfully achieving quantum-classical heterogeneous communication. In 2017, Shukla et al. [21] introduced an SQD protocol based on entangled Bell states for the first time. The classical party, Bob, had to perform permutations on photon sequences and publish permutation operators, which not only increased investment costs for the classical side but also reduced communication efficiency. Therefore, reducing resource consumption and improving communication efficiency became primary concerns for researchers. In terms of conserving quantum resources, Rong et al. [22] proposed a mediated semi-quantum secure direct communication protocol in 2021, enabling two classical users to transmit secret information with the assistance of a fully quantum third party. This significantly reduced the reliance on quantum devices. To enhance efficiency, Shi [23] constructed an efficient SQD protocol in 2023 based on polarization-spatial mode hyperentangled Bell states, achieving a transmission efficiency of 50%. In 2025, Li et al. [24] proposed an SQD protocol based on four-particle Omega states, which achieves significantly enhanced trans-

mission efficiency while ensuring security, opening new dimensions for SQD research. That same year, Zhang et al. [25] designed a d-dimensional single-particle-state-based SQD protocol through groundbreaking simplification of semi-quantum operations. This approach requires only particle permutation operations, eliminating the need for quantum state preparation or measurement steps essential in conventional protocols.

Based on the analysis provided, this paper proposes a novel protocol designated as multi-party controlled semi-quantum dialogue (MCSQD) based on hyperentangled Bell states. In this protocol, multi-party controllers are capable of simultaneously controlling the participating parties, preventing communication without their permission. The classical party employs Huffman compression technology for encoding before sending information to the quantum party. Similarly, Alice uses compression techniques to encode source information into binary strings. Leveraging unitary operations, Alice can encode string onto the code particles. Bob decodes to obtain the secret message based on the measurement results announced by Alice. By introducing Huffman compression coding technology, the storage space complexity for the participants can be significantly optimized. Furthermore, the protocol exhibits exceptional robustness against prevalent external and internal attack vectors, providing strong support for complex-scenario CSQD.

The structure of the paper is organized as follows: Section 2 introduces the relevant theoretical knowledge and details the design of the MCSQD protocol; Section 3 analyzes the security of the MCSQD protocol; Section 4 calculates and compares the communication efficiency of the protocol; and Section 5 concludes the findings and contributions of the work.

2. MCSQD Protocol

2.1. Preliminary Preparations

2.1.1. Preparation of Quantum States

In the proposed MCSQD protocol, the controller Charlie_i and Alice possess full quantum capabilities. In contrast, participant Bob is classical, meaning he can only perform the following classical operations:

(1) Measure and prepare qubits exclusively in the Z-basis;
(2) Reflect qubits to other participants without any disturbance;
(3) Reorder qubits using different delay lines.

Charlie_1 is responsible for preparing N identical hyperentangled photon pairs in the polarization-spatial mode:

$$|\Phi\rangle_{AB}^{PS} = |\eta\rangle_{AB}^{P} \otimes |\xi\rangle_{AB}^{S} \tag{1}$$

where the subscripts A and B denote two distinct photons in the system, and the superscripts P and S represent the polarization DOF and the spatial DOF, respectively. $|\eta\rangle_{AB}^{P} \in \left\{|\varphi^{\pm}\rangle^{P}, |\psi^{\pm}\rangle^{P}\right\}$, $|\xi\rangle_{AB}^{S} \in \left\{|\varphi^{\pm}\rangle^{S}, |\psi^{\pm}\rangle^{S}\right\}$. This can be specifically expressed as:

$$\begin{aligned}
|\varphi^{\pm}\rangle^{P} &= \frac{1}{\sqrt{2}}(|\mathrm{HH}\rangle \pm |\mathrm{V}V\rangle)^{P} \\
|\psi^{\pm}\rangle^{P} &= \frac{1}{\sqrt{2}}(|\mathrm{HV}\rangle \pm |\mathrm{V}H\rangle)^{P} \\
|\varphi^{\pm}\rangle^{S} &= \frac{1}{\sqrt{2}}(|a_1b_1\rangle \pm |a_2b_2\rangle)^{S} \\
|\psi^{\pm}\rangle^{S} &= \frac{1}{\sqrt{2}}(|a_1b_2\rangle \pm |a_2b_1\rangle)^{S}
\end{aligned} \tag{2}$$

Here, H and V represent the horizontal and vertical polarization states of the hyperentangled photon pair, while $a_1, a_2(b_1, b_2)$ denote the distinct spatial modes of photon A(B). In 2005, the Yang team [26] successfully prepared hyperentangled two-photon states in both polarization and spatial DOF by exciting a β-barium borate (BBO) crystal with femtosecond pump pulses. Subsequent advancements in quantum optical technology have enabled full discrimination of hyperentangled states [27,28], with extensive applications across quantum information processing domains including entanglement purification, concentration protocols, and Bell-state analysis.

During the measurement process, several measurement bases are utilized, including Z_P, X_P, and $Z_M = Z_P \otimes Z_S$. Specifically, for the polarization DOF:

$$Z_P = \{|\mathrm{H}\rangle, |\mathrm{V}\rangle\}$$

$$X_P = \{|+_P\rangle = \frac{1}{\sqrt{2}}(|\mathrm{H}\rangle + |V\rangle), |-_P\rangle = \frac{1}{\sqrt{2}}(|\mathrm{H}\rangle - |V\rangle)\} \tag{3}$$

In the spatial-mode DOF, $Z_S \in \{Z_{SA}, Z_{SB}\}$, where:

$$Z_{SA} = \{|a_1\rangle, |a_2\rangle\}$$

$$Z_{SB} = \{|b_1\rangle, |b_2\rangle\} \tag{4}$$

To address the question of how to select Z_S for measurement, Alice (or Bob) will choose an appropriate measurement basis based on the photon sequence in their possession. For instance, if Bob wishes to determine the quantum state of particle B in the spatial-mode DOF within S_B, he will select the Z_{SB} measurement basis.

Compared to most previous SQD protocols, the proposed protocol introduces significant improvements in the encoding method by adopting an adaptive Huffman compression coding algorithm. This approach constructs a Huffman tree to assign values to each character, markedly optimizing the storage space complexity for classical parties. The classical party leverages an "immediate measurement and transmission" mechanism, enabling it to complete encoding and decoding operations without temporarily storing qubits. Utilizing Huffman compression coding for information transmission greatly reduces the storage space required on the classical side, enhancing communication efficiency in semi-quantum secure dialogue.

2.1.2. Huffman Compression Coding

Huffman compression coding [29] is a classical lossless data compression algorithm. Its core mechanism constructs an optimal prefix binary tree that assigns shorter codewords to high-frequency characters and longer codewords to low-frequency characters, thereby reducing overall data storage requirements. As a fundamental and pivotal tree data structure, a binary tree is characterized by its defining property where each node possesses at most two child nodes (conventionally termed the left child node and right child node). Arithmetic coding [30] might offer higher compression ratios but comes with increased complexity, whereas Huffman coding is relatively simple to implement and suitable for many practical systems. To ensure efficient data transmission between the classical party and the quantum party while balancing cost constraints and classical-side equipment limitations, the protocols can employ Huffman compression coding to reduce data volume. Notably, Huffman compression coding introduces no additional security vulnerabilities, while its prefix-free code property synergizes effectively with quantum error detection mechanisms. The specific steps are outlined below:

(1) Frequency Calculation: First, calculate the frequency of each character in the data to be compressed. For example, in the string "$xyzxyzxxpq$" that Bob intends to transmit, the frequencies of the characters are as follows: $P(m_i = x) = 0.4$, $P(m_i = y) = P(m_i = z) = 0.2$, and $P(m_i = p) = P(m_i = q) = 0.1$.

(2) Building the Huffman Tree: Treat each character and its frequency as a leaf node and arrange them in ascending order of frequency. Repeat the following steps until only one root node remains:

1. Extract the two nodes with the smallest frequencies, merge them into a new node, and set the frequency of the new node as the sum of the two frequencies.
2. Reinsert the new node back into the queue.

The final tree formed through this process is the Huffman tree. The path from the root node to each leaf node determines the binary encoding of the corresponding character.

(3) Assigning Codes: Starting from the root node, assign a '0' for moving to the left subtree and a '1' for moving to the right subtree. The binary sequence along the path from the root node to a specific character represents the encoding of that character. Figure 1 illustrates the Huffman tree constructed using the string "$xyzxyzxxpq$" as an example.

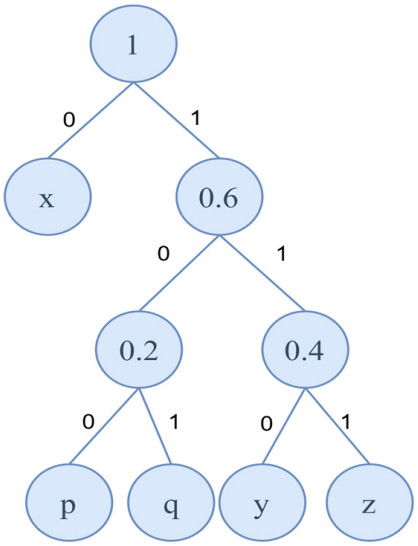

Figure 1. Example of a Huffman Tree Diagram.

Based on the Huffman tree, we can obtain the corresponding binary codes for each character in the string "$xyzxyzxxpq$", as shown in Table 1.

Table 1. Binary codes corresponding to each character.

Character Values	Binary Encoding
x	0
y	110
z	111
p	100
q	101

2.2. Protocol Process

Step 1: Charlie$_1$ prepares N identical hyperentangled photon pairs in the polarization-spatial mode, denoted as $|\Phi\rangle_{AB}^{PS} = |\varphi^+\rangle^P \otimes |\varphi^+\rangle^S$. The particles A and B are separated to form sequences S_A and S_B, respectively. Subsequently, Charlie$_1$ randomly applies unitary operations $R = \{I, X, H\}$ for the first n($\mathrm{n} < N$) particles in S_A at each DOF. The sequence S_A is then sequentially transmitted to Charlie$_2$, Charlie$_3$, ..., Charlie$_\mathrm{n}$, while recording the operations performed. Charlie$_\mathrm{n}$ sends S_A to the quantum party Alice and retains S_B.

Step 2: To prevent Trojan horse attacks [31–33], Alice and Bob place a photon number splitter (PNS) and a wavelength filter [20] in front of their devices. Upon confirming the receipt of the sequence by Alice, she randomly selects a sufficient number of particles from the remaining $N - n$ in the S_A to serve as decoy particles for security checks. Alice measures these particles using either the Z basis or X basis across the two DOF and collaborates with Charlie$_\mathrm{n}$ to calculate the quantum bit error rate (QBER). If the error rate is below a pre-defined threshold, Alice removes the decoy particles. Subsequently, the controllers execute hierarchical authorization, requiring all independent controllers Charlie$_\mathrm{i}$($i = 1, \ldots, n$) to collectively authorize permission for Alice and Bob to communicate. Alice applies the same unitary operation R to recover the initial hyperentangled state $|\Phi\rangle_{AB}^{PS}$. Finally, Charlie$_\mathrm{n}$ transmits S_B to Bob. Charlie$_\mathrm{i}$($i = 1, \ldots, n$) will not publish or send any information if communication is not permitted.

Step 3: After confirming that Bob has received the sequence, Bob initiates measurements on the first n particles of S_B using the measurement basis $Z_M = Z_P \otimes Z_S$. Subsequently, Bob employs Huffman compression coding to compress the source information m_B into a binary sequence M_B. Based on the value of each bit M_B^i, Bob prepares corresponding qubits in the two DOF. If $M_B^i = 0$, Bob prepares the same quantum state in the respective DOF; otherwise, he prepares the opposite quantum state. For example, if $M_B = 001011$, Bob will sequentially prepare separable single-photon states: $|\mathrm{H}\rangle^P|b_1\rangle^S$, $|\mathrm{V}\rangle^P|b_1\rangle^S$, and $|\mathrm{V}\rangle^P|b_2\rangle^S$, which are then sent to Alice as Code particles. From the remaining $N - n$ particles, Bob selects decoy particles for the subsequent security check and reflects them directly to Alice as Reflect particles. Once ready, Bob reorders and records the Reflect and Code particles before transmitting them to Alice.

Step 4: Bob first announces the correct order of the Reflect particles. Alice performs measurements on these particles and collaborates with Charlie$_\mathrm{n}$ to calculate the QBER. If the error rate is below a pre-defined threshold, Alice removes the Reflect particles.

Step 5: Bob then announces the correct order of the Code particles. Alice restores the order and measures the Code particles along with her retained S_A using the measurement basis $Z_M = Z_P \otimes Z_S$ to obtain M_B. Finally, Alice applies Huffman decompression to recover the original source information m_B. To facilitate the conversation, Alice also encodes her secret message m_A using Huffman compression into a binary string M_A. Subsequently, she performs the corresponding unitary operations for encoding based on the value of M_A ($00 \rightarrow I^P \otimes I^S$, $01 \rightarrow I^P \otimes \sigma_X^S$, $10 \rightarrow \sigma_X^P \otimes I^S$, $11 \rightarrow \sigma_X^P \otimes \sigma_X^S$). After encoding, she performs measurements and publishes the results. Bob can easily obtain Alice's secret message m_A by using the measurement results announced by Alice and performing decompression. The schematic diagram of the MCSQD protocol is shown in Figure 2.

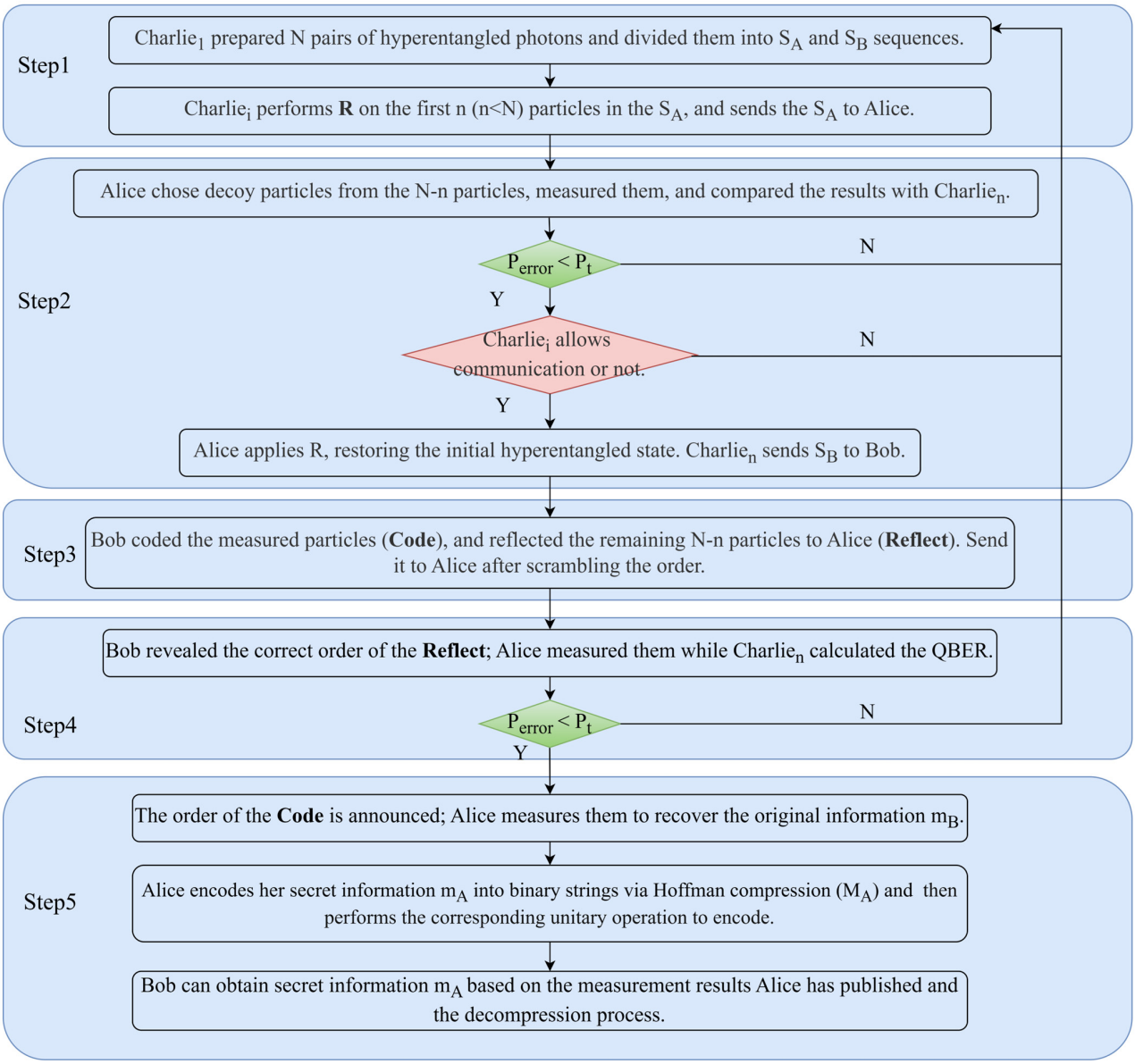

Figure 2. Schematic diagram of the MCSQD protocol.

3. Security Analysis

3.1. The Trojan Horse Attack

Since the proposed MCSQD protocol is bidirectional, it is necessary to consider Trojan horse attacks [31–33]. In this scenario, Eve generates spy photons and injects them into the transmitted sequences S_A and S_B to perform invisible photon attacks. Eve captures the sequences and then separates and measures the encrypted spy photons to steal information from Alice and Bob while forwarding the remaining legitimate particles to the controller Charlie$_n$. To counteract such attacks, in Step 2 of the proposed protocol, Alice(Bob) has already installed a PNS: 50/50 and a wavelength filter before receiving the sequences $S_A(S_B)$. The PNS can be used to protect against delayed photon attacks by checking for the presence of multi-photon signals, and the quantum wavelength filter removes illegal photons under invisible photon attacks. This setup effectively resists the Trojan horse attack.

3.2. The Measure-Resend Attack

Eve intercepts and measures the sequence S_B sent by Charlie$_n$ to Bob, then prepares and sends fake qubits to Bob based on her measurement results. This allows Eve to steal

Bob's bit string M_B without being detected. However, in Step 3 of the protocol, Bob randomly selects a sufficient number of particles from S_B to serve as decoy particles for the second security check and shuffles their order. Consequently, Eve cannot determine the exact positions of the decoy particles or the required measurement bases. When considering the polarization DOF, Eve randomly selects either Z_P or X_P for measurement. The probability that Eve remains undetected is calculated as: $\frac{1}{2} \times 1 + \frac{1}{2} \times \frac{1}{2} = \frac{3}{4}$. In a system involving both polarization and spatial-mode DOF, the final probability of detection is: $1 - (\frac{3}{4})^{2d}$, where d represents the number of decoy particles. When d is sufficiently large, the error rate will exceed a predefined threshold, ensuring detection. Based on the above discussion, the protocol effectively defends against the measure-resend attack.

3.3. The Entangle-Measure Attack

The entangle-measure attack refers to the scenario where Eve uses a unitary operation $\hat{E}$ to entangle an auxiliary particle $|\varepsilon\rangle_e$, which she has prepared, with the intercepted sequence of S_B particles. Subsequently, when Bob completes his encoding and transmits the particles to Alice, Eve intercepts them again and applies another unitary operation $\hat{F}$. Finally, by measuring her auxiliary particle $|\varepsilon\rangle_e$, Eve attempts to infer useful information.

$$\hat{E} = \begin{pmatrix} \alpha_1 & \beta_2 \\ \beta_1 & \alpha_2 \end{pmatrix} \bigotimes \begin{pmatrix} \alpha_1{}' & \beta_2{}' \\ \beta_1{}' & \alpha_2{}' \end{pmatrix} \tag{5}$$

Assuming the initial state of the system is $|\Phi\rangle_{AB}^{PS} = |\varphi^+\rangle^P \otimes |\varphi^+\rangle^S$, the composite state of the system after Eve performs the entanglement operation becomes:

$$\begin{aligned}
\hat{E}|\varphi^+\rangle^P \otimes |\varphi^+\rangle^S|\varepsilon\rangle_e = {} & \frac{1}{\sqrt{2}}\left[|\mathrm{H}\rangle_A(\alpha_1|\mathrm{H}\rangle_B|\varepsilon_{00}\rangle_e + \beta_1|\mathrm{V}\rangle_B|\varepsilon_{01}\rangle_e) + |\mathrm{V}\rangle_A(\beta_2|\mathrm{H}\rangle_B|\varepsilon_{10}\rangle_e + \alpha_2|\mathrm{V}\rangle_B|\varepsilon_{11}\rangle_e)\right]^P \\
& \otimes \frac{1}{\sqrt{2}}\left[|a_1\rangle_A(\alpha_1{}'|b_1\rangle_B|\varepsilon_{00}\rangle_e + \beta_1{}'|b_2\rangle_B|\varepsilon_{01}\rangle_e) + |a_2\rangle_A(\beta_2{}'|b_1\rangle_B|\varepsilon_{10}\rangle_e + \alpha_2{}'|b_2\rangle_B|\varepsilon_{11}\rangle_e)\right]^S \\
= {} & \frac{1}{\sqrt{2}}\left[|\mathrm{H}\rangle_B(\alpha_1|\mathrm{H}\rangle_A|\varepsilon_{00}\rangle_e + \beta_2|\mathrm{V}\rangle_A|\varepsilon_{10}\rangle_e) + |\mathrm{V}\rangle_B(\beta_1|\mathrm{H}\rangle_A|\varepsilon_{01}\rangle_e + \alpha_2|\mathrm{V}\rangle_A|\varepsilon_{11}\rangle_e)\right]^P \\
& \otimes \frac{1}{\sqrt{2}}[|b_1\rangle_B(\alpha_1{}'|a_1\rangle_A|\varepsilon_{00}\rangle_e + \beta_2{}'|a_2\rangle_A|\varepsilon_{10}\rangle_e) + |b_2\rangle_B(\beta_1{}'|a_1\rangle_A|\varepsilon_{01}\rangle_e \\
& + \alpha_2{}'|a_2\rangle_A|\varepsilon_{11}\rangle_e)]^S
\end{aligned} \tag{6}$$

$[|\varepsilon_{00}\rangle, |\varepsilon_{01}\rangle, |\varepsilon_{10}\rangle, |\varepsilon_{11}\rangle]^{P/S}$ belongs to the Hilbert space of Eve's probe states. Clearly, these states must satisfy the condition: $\hat{E}^\dagger\hat{E} = \hat{E}\hat{E}^\dagger = I$.

$$\begin{aligned}
&[\langle\varepsilon_{00}|\varepsilon_{00}\rangle + \langle\varepsilon_{01}|\varepsilon_{01}\rangle]^{P/S} = 1 \\
&[\langle\varepsilon_{10}|\varepsilon_{10}\rangle + \langle\varepsilon_{11}|\varepsilon_{11}\rangle]^{P/S} = 1 \\
&[\langle\varepsilon_{00}|\varepsilon_{10}\rangle + \langle\varepsilon_{01}|\varepsilon_{11}\rangle]^{P/S} = 0
\end{aligned} \tag{7}$$

Since $\hat{E}$ represents Eve's unitary operation, it must satisfy the following equation:

$$\begin{aligned}
&|\alpha_i|^2 + |\beta_i|^2 = 1,\ |\alpha_1|^2 = |\alpha_2|^2 \text{and } |\beta_1|^2 = |\beta_2|^2 \\
&|\alpha_i{}'|^2 + |\beta_i{}'|^2 = 1,\ |\alpha_1{}'|^2 = |\alpha_2{}'|^2 \text{and } |\beta_1{}'|^2 = |\beta_2{}'|^2
\end{aligned} \tag{8}$$

① In Step 3, after Bob measures the target particles to be encoded using the measurement basis $Z_M = Z_P \otimes Z_S$, the composite system collapses into a state $|\Phi'\rangle_{ABe}^{PS}$. This state is one of the following possibilities:

$$[|\mathrm{H}\rangle_B(\alpha_1|\mathrm{H}\rangle_A|\varepsilon_{00}\rangle_e + \beta_2|\mathrm{V}\rangle_A|\varepsilon_{10}\rangle_e)]^P \otimes [|b_1\rangle_B(\alpha_1{}'|a_1\rangle_A|\varepsilon_{00}\rangle_e + \beta_2{}'|a_2\rangle_A|\varepsilon_{10}\rangle_e)]^S$$

$$[|\mathrm{H}\rangle_B(\alpha_1|\mathrm{H}\rangle_A|\varepsilon_{00}\rangle_e+\beta_2|\mathrm{V}\rangle_A|\varepsilon_{10}\rangle_e)]^P\otimes\left[|b_2\rangle_B(\beta_1{}'|a_1\rangle_A|\varepsilon_{01}\rangle_e+\alpha_2{}'|a_2\rangle_A|\varepsilon_{11}\rangle_e)\right]^S$$
$$[|\mathrm{V}\rangle_B(\beta_1|\mathrm{H}\rangle_A|\varepsilon_{01}\rangle_e+\alpha_2|\mathrm{V}\rangle_A|\varepsilon_{11}\rangle_e)]^P\otimes\left[|b_1\rangle_B(\alpha_1{}'|a_1\rangle_A|\varepsilon_{00}\rangle_e+\beta_2{}'|a_2\rangle_A|\varepsilon_{10}\rangle_e)\right]^S$$
$$[|\mathrm{V}\rangle_B(\beta_1|\mathrm{H}\rangle_A|\varepsilon_{01}\rangle_e+\alpha_2|\mathrm{V}\rangle_A|\varepsilon_{11}\rangle_e)]^P\otimes\left[|b_2\rangle_B(\beta_1{}'|a_1\rangle_A|\varepsilon_{01}\rangle_e+\alpha_2{}'|a_2\rangle_A|\varepsilon_{11}\rangle_e)\right]^S \quad (9)$$

When Bob completes his encoding and sends the particles to Alice, Eve intercepts them again and applies another unitary operation $\hat{F}$. The state is then updated to:

$$\hat{F}\left|\Phi'\right\rangle_{ABe}^{PS}|\delta\rangle_e=\left|\Phi''\right\rangle_{ABe}^{PS} \quad (10)$$

Specifically:

$$\hat{F}[|\mathrm{H}\rangle_B(\alpha_1|\mathrm{H}\rangle_A|\varepsilon_{00}\rangle_e+\beta_2|\mathrm{V}\rangle_A|\varepsilon_{10}\rangle_e)]^P\otimes\left[|b_1\rangle_B(\alpha_1{}'|a_1\rangle_A|\varepsilon_{00}\rangle_e+\beta_2{}'|a_2\rangle_A|\varepsilon_{10}\rangle_e)\right]^S$$
$$=\left[\alpha_1|\mathrm{H}\rangle_A|\mathrm{H}\rangle_B|\delta_{00}\rangle_e+\beta_2|\mathrm{V}\rangle_A|\mathrm{H}\rangle_B|\delta_{10}\rangle_e\right]^P$$
$$\otimes\left[\alpha_1{}'|a_1\rangle_A|b_1\rangle_B|\delta_{00}\rangle_e+\beta_2{}'|a_2\rangle_A|b_1\rangle_B|\delta_{10}\rangle_e\right]^S \quad (11)$$

If Eve aims to execute a perfect entangle-measure attack without being detected by the legitimate parties, the state in Equation (11) will collapse into the following form:

$$\left[|\mathrm{H}\rangle_A|\mathrm{H}\rangle_B|\delta_{00}\rangle_e\right]^P\otimes\left[|a_1\rangle_A|b_1\rangle_B|\delta_{00}\rangle_e\right]^S \quad (12)$$

with the conditions:

$$\alpha_1=\alpha_1{}'=1,\beta_2=\beta_2{}'=0 \quad (13)$$

Similarly, for the remaining three cases in Equation (9), analogous results can be obtained, such as:

$$\alpha_1=\alpha_2{}'=1,\beta_2=\beta_1{}'=0$$
$$\alpha_2=\alpha_1{}'=1,\beta_1=\beta_2{}'=0$$
$$\alpha_2=\alpha_2{}'=1,\beta_1=\beta_1{}'=0 \quad (14)$$

② If Eve intercepts the Reflect particles and applies two unitary operations, $\hat{E}$ and $\hat{F}$, the state of the system will undergo transformations as follows:

$$\hat{E}\hat{F}\left|\varphi^+\right\rangle^P\otimes\left|\varphi^+\right\rangle^S|\varepsilon\rangle_e=\frac{1}{\sqrt{2}}[|\mathrm{H}\rangle_A(\alpha_1|\mathrm{H}\rangle_B|\delta_{00}\rangle_e+\beta_1|\mathrm{V}\rangle_B|\delta_{01}\rangle_e)+|\mathrm{V}\rangle_A(\beta_2|\mathrm{H}\rangle_B|\delta_{10}\rangle_e+\alpha_2|\mathrm{V}\rangle_B|\delta_{11}\rangle_e)]^P$$
$$\otimes\frac{1}{\sqrt{2}}[|a_1\rangle_A(\alpha_1{}'|b_1\rangle_B|\delta_{00}\rangle_e+\beta_1{}'|b_2\rangle_B|\delta_{01}\rangle_e)+|a_2\rangle_A(\beta_2{}'|b_1\rangle_B|\delta_{10}\rangle_e$$
$$+\alpha_2{}'|b_2\rangle_B|\delta_{11}\rangle_e)]^S \quad (15)$$

It also satisfies Equations (8), (13), and (14):

$$\hat{E}\hat{F}\left|\varphi^+\right\rangle^P\otimes\left|\varphi^+\right\rangle^S|\varepsilon\rangle_e=\frac{1}{\sqrt{2}}(|\mathrm{H}\rangle_A|\mathrm{H}\rangle_B|\delta_{00}\rangle_e+|\mathrm{V}\rangle_A|\mathrm{V}\rangle_B|\delta_{11}\rangle_e)^P$$
$$\otimes\frac{1}{\sqrt{2}}(|a_1\rangle_A|b_1\rangle_B|\delta_{00}\rangle_e+|a_2\rangle_A|b_2\rangle_B|\delta_{11}\rangle_e)^S \quad (16)$$

From the transformation of Equation (2), we know that:

$$|\mathrm{HH}\rangle^P=\frac{1}{\sqrt{2}}(\left|\varphi^+\right\rangle^P+\left|\varphi^-\right\rangle^P)$$
$$|\mathrm{V}V\rangle^P=\frac{1}{\sqrt{2}}(\left|\varphi^+\right\rangle^P-\left|\varphi^-\right\rangle^P)$$

$$|a_1 b_1\rangle^P = \frac{1}{\sqrt{2}}(|\varphi^+\rangle^S + |\varphi^-\rangle^S)$$
$$|a_2 b_2\rangle^P = \frac{1}{\sqrt{2}}(|\varphi^+\rangle^S - |\varphi^-\rangle^S) \quad (17)$$

Substituting Equation (17) into Equation (16), we obtain:

$$\hat{E}\hat{F}\,|\,\varphi^+\rangle^P \otimes |\,\varphi^+\rangle^S|\varepsilon\rangle_e = \frac{1}{2}[|\varphi^+\rangle^P(|\delta_{00}\rangle_e + |\delta_{11}\rangle_e)^P + |\varphi^-\rangle^P(|\delta_{00}\rangle_e - |\delta_{11}\rangle_e)^P]$$
$$\otimes\frac{1}{2}\Big[|\varphi^+\rangle^S(|\delta_{00}\rangle_e + |\delta_{11}\rangle_e)^S + |\varphi^-\rangle^S(|\delta_{00}\rangle_e - |\delta_{11}\rangle_e)^S \quad (18)$$

Similarly, for Eve to avoid detection during this entangle-measure attack, Equation (18) must satisfy the following conditions:

$$|\delta_{00}\rangle_e{}^P = |\delta_{11}\rangle_e{}^P, |\delta_{00}\rangle_e{}^S = |\delta_{11}\rangle_e{}^S \quad (19)$$

In summary, it is not difficult to conclude that, regardless of whether the attack occurs in the polarization DOF or the spatial-mode DOF, Eve cannot distinguish between the states $|\varepsilon_{ij}\rangle^{P/S}$. This means that Eve cannot obtain any useful information. Therefore, the protocol demonstrates robustness against the entangle-measure attack. Figure 3 shows a schematic diagram of the entangle-measure attack.

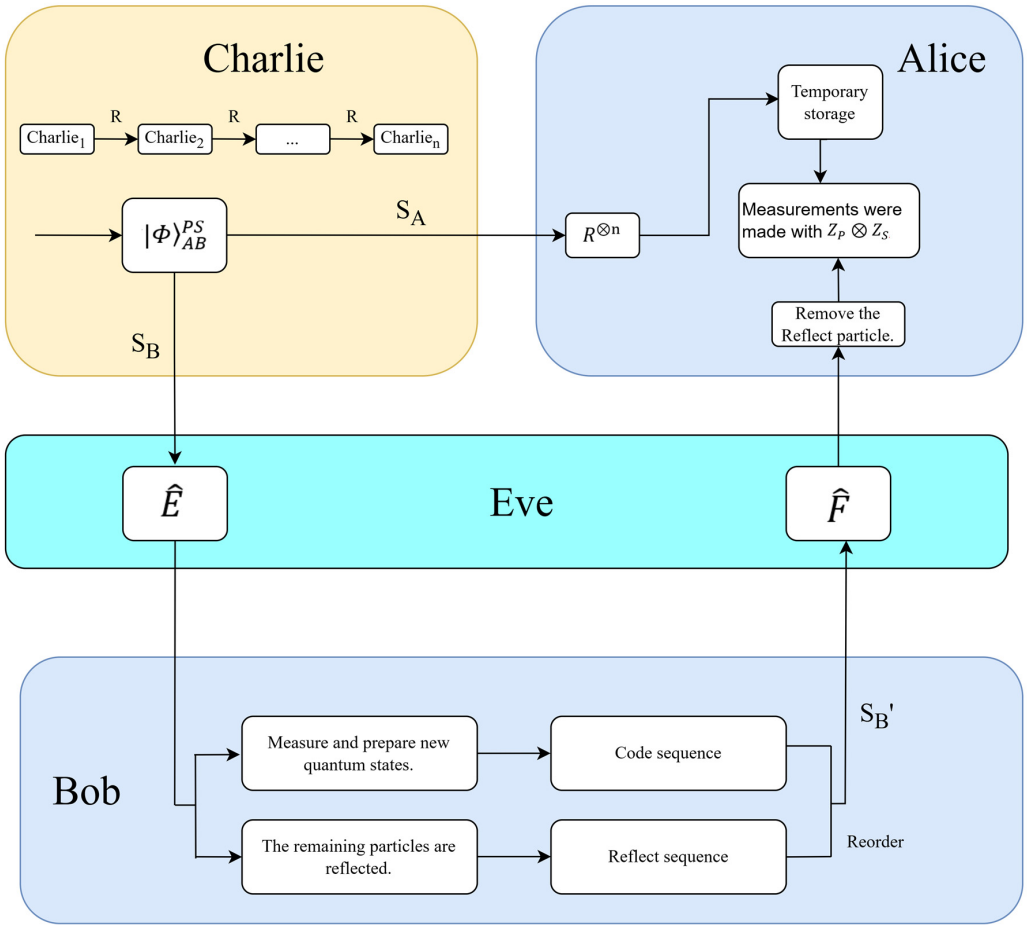

Figure 3. Schematic diagram of the entangle-measure attack.

3.4. Attacks by the Dishonest Controller

Compared to external attacks initiated by an eavesdropper like Eve, internal attacks by a dishonest controller are more severe. In the MCSQD system, the controller acts as a core

component responsible for coordinating the communication process among participants. If the controller behaves dishonestly, it poses a significant threat to the overall security of the communication system. The following analysis explores specific methods of attack by a dishonest controller.

3.4.1. Entanglement Substitution

A dishonest controller Charlie_1 does not prepare the agreed-upon hyperentangled Bell state $|\Phi\rangle_{AB}^{PS} = |\varphi^+\rangle^P \otimes |\varphi^+\rangle^S$ but instead uses a different hyperentangled state $|\Phi\rangle_{ABC}^{PS}$.

$$|\Phi\rangle_{ABC}^{PS} = \frac{1}{\sqrt{2}}(|\text{HHH}\rangle + |\text{VVV}\rangle)_{ABC}^{P} \otimes \frac{1}{\sqrt{2}}(|a_1 b_1 c_1\rangle + |a_2 b_2 c_2\rangle)_{ABC}^{S} \tag{20}$$

Subsequently, Charlie_n sends the sequence S_A to Alice and S_B to Bob. Charlie_n then attempts to steal Alice and Bob's secret messages by measuring the sequence S_C using the measurement basis. However, in Step 3, Bob prepares new qubits based on the string to be transmitted and uses a permutation operator to shuffle the order of the particles. This shuffling prevents Charlie_n from knowing the quantum states of the encoded Code particles. Consequently, Charlie_n cannot deduce Bob's secret information M_B.

3.4.2. Operation Tampering

A malicious controller Charlie_i could deliberately broadcast erroneous unitary operations R_1 to disrupt the communication process. If Alice does not recover the correct initial state due to this misinformation, it will result in discrepancies during subsequent measurements, preventing her from correctly comparing the outcomes with the initial system state. If Charlie_i publishes an erroneous unitary operation R_1, Alice will be unable to accurately restore the initial hyperentangled state prepared by Charlie_1. During the verification phase, when Alice and Charlie_n compare their measurement results, the QBER will be higher than the pre-defined threshold due to the mismatch caused by the incorrect operation. This high QBER indicates potential tampering or errors in the protocol, leading to the termination of the protocol. Consequently, Charlie_i will not be able to obtain any useful secret messages from Alice or Bob.

3.4.3. Deliberate Disclosure

When compromised controllers (e.g., Charlie_i) collude with external attacker Eve, they may leak operational parameters R to facilitate secret theft. The attack proceeds as follows: Eve intercepts particle sequence S_A sent from Charlie_n to Alice, forging a counterfeit sequence $S_A\prime$ to transmit to Alice. If all controllers are untrustworthy and disclose their operations $\{R_i\}$ to Eve, she may deduce the initial system state $|\Phi\rangle_{AB}^{PS}$ through reverse engineering to extract secrets. In Step 2 of the protocol, Alice selects sufficient particles from the remaining $N - n$ received sequences for security verification. Since Eve learns the system state after sending $S_A\prime$, she cannot predict Alice's chosen measurement basis. This inevitably triggers a QBER exceeding the predefined security threshold, forcing communication termination. As a result, the collusion between the controller and Eve will inevitably be detected.

3.5. Attack by the Dishonest Party

Typically, an attack by a dishonest participant, also known as a collusion attack, involves two parties attempting to bypass the control imposed by the controller, aiming to communicate directly without the controller's permission. However, in the proposed MCSQD protocol, before the hyperentangled state sequences are distributed, the A particles in sequence S_A undergo unitary operations $R = \{I, X, H\}$ by multi-party controllers to

encode control information. Therefore, without the controller's permission, the encoded particles lose their original correlations, making it impossible for the participants to deduce the correct secret information.

4. Efficiency Analysis

Quantum communication systems rely on rare and expensive quantum resources. Improving efficiency means transmitting more information while maintaining the same level of resource consumption, thereby optimizing resource utilization and minimizing costs. The information-theoretic efficiency defined in reference [34] is given by:

$$\eta = \frac{c}{q + b} \tag{21}$$

where c represents the number of bits used to transmit secret messages, q denotes the total number of qubits employed in the protocol, and b indicates the number of classical bits consumed. Notably, decoy qubits employed for eavesdropping detection are excluded from this calculation. As Feng et al. [35] demonstrated that when the number of decoy particles reaches 20, the probability of detecting an eavesdropper approaches 100%. In the proposed protocol's large-scale data transmission, decoy particle quantities exhibit negligible impact on total efficiency and are therefore omitted from the efficiency analysis. The total number of qubits consumed in the protocol is $q = 4n$, which includes: n pairs of hyperentangled photon prepared by Charlie_1, and $2n$ new separable single-photon qubits prepared by Bob in Step 3. During the transmission process, Bob needs to announce the correct order of the permutation operators, which consumes $2n$ classical bits. Therefore, $b = 2n$. The protocol successfully transmits $c = 4n$ secret message bits. Substituting these values into Equation (21), the efficiency of the protocol is calculated as: $\eta = \frac{4n}{4n+2n} = 66.7\%$.

A comparison of the proposed MCSQD protocol with related SQD protocols is shown in Table 2. It is evident that the proposed protocol achieves a relatively high communication efficiency. Moreover, it is suitable for a wide range of complex scenarios and offers significantly richer functionality compared to the SQD protocols listed in the table.

Table 2. Efficiency comparison.

Protocols	The Quantum State Used	c	q	b	η
Shukla [21]	Bell States	$2n$	$3n$	$3n$	50%
Zhou [36]	GHZ State	$3n$	$5n$	0	60%
Pan [37]	Bell States	$2n$	$4n$	$2n$	33.3%
Shi [23]	Hyperentangled Bell States	$2n$	$3n$	n	50%
Shi [38]	Bell States	$2n$	$4n$	n	50%
MCSQD	Hyperentangled Bell States	$4n$	$4n$	$2n$	66.7%

5. Conclusions

This study presents a novel multi-party controlled semi-quantum dialogue protocol based on hyperentangled Bell states. Within the protocol, Alice and Bob first apply classical data compression techniques to reduce redundancy. Subsequently, they employ quantum state encoding methods to map the compressed information onto hyperentangled Bell states within the polarization-spatial mode DOF. The multi-party controllers implement hierarchical authorization, permitting communication between participants only when all controllers concur on authorization. The introduction of Hoffman compression encoding, especially for the device-constrained classical party, can greatly save the physical storage space of the participants. Security analysis demonstrates that the protocol is robust against both common external and internal attacks posed by dishonest participants or controllers.

Compared to existing SQD protocols, the proposed MCSQD protocol exhibits significant advantages in terms of resource conservation and transmission efficiency. Although the generation of hyperentangled states presents some challenges, the protocol remains feasible with current technology, thereby offering promising prospects for practical applications.

Author Contributions: Methodology, M.-N.Z.; Software, Y.-H.F.; Validation, R.-G.Z. and Y.-H.F.; Formal analysis, M.-N.Z.; Investigation, M.-N.Z.; Resources, Y.-H.F.; Data curation, Y.-H.F.; Writing—original draft, M.-N.Z.; Writing—review & editing, R.-G.Z.; Visualization, M.-N.Z. and Y.-H.F.; Supervision, R.-G.Z.; Project administration, R.-G.Z.; Funding acquisition, R.-G.Z. All authors have read and agreed to the published version of the manuscript.

Funding: This work is supported by the National Natural Science Foundation of China under Grant Nos. 62172268 and 62302289, and the Shanghai Science and Technology Project under Grant No. 23YF1416200.

Institutional Review Board Statement: Not applicable.

Data Availability Statement: Data are contained within the article.

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

References

1. Long, G.L.; Liu, X.S. Theoretically efficient high-capacity quantum-key-distribution scheme. *Phys.Rev. A* **2002**, *65*, 032302. [CrossRef]
2. Deng, F.G.; Long, G.L.; Liu, X.S. Two-step quantum direct communication protocol using the EinsteinPodolsky-Rosen pair block. *Phys. Rev. A* **2003**, *68*, 042317. [CrossRef]
3. Zhou, Z.R.; Sheng, Y.B.; Niu, P.H.; Yin, L.G.; Long, G.L.; Hanzo, L. Measurement-device-independent quantum secure direct communication. *Sci. China Phys. Mech. Astron.* **2020**, *63*, 230362. [CrossRef]
4. Wu, X.D.; Zhou, L.; Zhong, W.; Sheng, Y.B. High-capacity measurement-device-independent quantum secure direct communication. *Quantum Inf. Process.* **2020**, *19*, 354. [CrossRef]
5. Zhu, F.; Zhang, W.; Sheng, Y.B.; Huang, Y.D. Experimental long-distance quantum secure direct communication. *Sci. Bull.* **2017**, *62*, 1519–1524. [CrossRef]
6. Qi, R.Y.; Sun, Z.; Lin, Z.S.; Niu, P.H.; Hao, W.T.; Song, L.Y.; Huang, Q.; Gao, J.C.; Yin, L.G.; Long, G.L. Implementation and security analysis of practical quantum secure direct communication. *Light Sci. Appl.* **2019**, *8*, 22. [CrossRef]
7. Qi, Z.T.; Li, Y.H.; Huang, Y.W.; Feng, J.; Zheng, Y.L.; Chen, X.F. A 15-user quantum secure direct communication network. *Light Sci. Appl.* **2021**, *10*, 183. [CrossRef]
8. Wang, M.; Zhang, W.; Guo, J.; Song, X.; Long, G. Experimental demonstration of secure relay in quantum secure direct communication network. *Entropy* **2023**, *25*, 1548. [CrossRef]
9. Nguyen, B.A. Quantum dialogue. *Phys. Lett. A* **2004**, *328*, 6–10. [CrossRef]
10. 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*, 559–566. [CrossRef]
11. Ye, T.Y. Quantum secure dialogue with quantum encryption. *Commun. Theor. Phys.* **2014**, *62*, 338. [CrossRef]
12. Yin, A.H.; Tang, Z.H.; Chen, D. Efficient quantum dialogue without information leakage. *Mod. Phys. Lett. B* **2015**, *29*, 1550018. [CrossRef]
13. Qi, J.M.; Xu, G.; Chen, X.B.; Wang, T.Y.; Cai, X.Q.; Yang, Y.X. Two authenticated quantum dialogue protocols based on three-particle entangled states. *Quantum Inf. Process.* **2018**, *17*, 247. [CrossRef]
14. Han, K.Q.; Zhou, L.; Zhong, W.; Sheng, Y.B. Measurement-device-independent quantum dialogue based on hyperentanglement. *Quantum Inf. Process.* **2021**, *20*, 280. [CrossRef]
15. Lin, J.; Chang, C.Y. Efficient fault-tolerant quantum dialogue protocols using a quantum reordering circuit of EPR pairs. *Phys. Scr.* **2023**, *98*, 095110. [CrossRef]
16. Zhu, P.H.; Zhong, W.; Du, M.M.; Li, X.Y.; Zhou, L.; Sheng, Y.B. One-step quantum dialogue. *Chin. Phys. B* **2024**, *33*, 030302. [CrossRef]
17. Wang, Y.; Yang, T.; Xu, J.; Chen, X. A dialogue protocol of quantum communication network based on cluster states. *Quantum Inf. Process.* **2024**, *23*, 13. [CrossRef]
18. Lang, Y.F.; Cai, C.C. Fast quantum dialogue. *EPJ Quantum Technol.* **2025**, *12*, 59. [CrossRef]

19. Huang, R.-C.; Yang, Y.-G.; Xu, G.-B.; Jiang, D.-H.; Zhou, Y.-H.; Shi, W.-M. Counterfactual controlled quantum dialogue protocol. *Quantum Inf. Process.* **2025**, *24*, 63. [CrossRef]
20. Boyer, M.; Gelles, R.; Kenigsberg, D.; Mor, T. Semi-quantum key distribution. *Phys. Rev. A* **2009**, *79*, 032341. [CrossRef]
21. 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]
22. Rong, Z.; Qiu, D.; Mateus, P.; Zou, X. Mediated semi-quantum secure direct communication. *Quantum Inf. Process.* **2021**, *20*, 58. [CrossRef]
23. Shi, G.F. Semi-quantum dialogue scheme based on hyperentangled Bell states. *Phys. Scr.* **2023**, *98*, 115120. [CrossRef]
24. 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]
25. Zhang, L.; Liu, X.; Xin, X.-J.; Li, P. Semi-Quantum Dialogue with d-Dimensional Single Particles. *Int. J. Theor. Phys.* **2025**, *64*, 133. [CrossRef]
26. Yang, T.; Zhang, Q.; Zhang, J.; Yin, J.; Zhao, Z.; Żukowski, M.; Pan, J.W. All-versus-nothing violation of local realism by two-photon, four-dimensional entanglement. *Phys. Rev. Lett.* **2005**, *95*, 240406. [CrossRef]
27. Sheng, Y.B.; Deng, F.G.; Long, G.L. Complete hyperentangled-Bell-state analysis for quantum communication. *Phys. Rev. A—At. Mol. Opt. Phys.* **2010**, *82*, 032318. [CrossRef]
28. Ren, B.C.; Wei, H.R.; Hua, M.; Li, T.; Deng, F.G. Complete hyperentangled-Bell-state analysis for photon systems assisted by quantum-dot spins in optical microcavities. *Opt. Express* **2012**, *20*, 24664–24677. [CrossRef]
29. Habib, A.; Rahman, M.S. Balancing decoding speed and memory usage for Huffman codes using quaternary tree. *Appl. Inform.* **2017**, *4*, 5. [CrossRef]
30. Chuang, I.L.; Modha, D.S. Reversible arithmetic coding for quantum data compression. *IEEE Trans. Inf. Theory* **2000**, *46*, 1104–1116. [CrossRef]
31. Li, X.H.; Deng, F.G.; Zhou, H.Y. Improving the security of secure direct communication based on the secret transmitting order of particles. *Phys. Rev. A—At. Mol. Opt. Phys.* **2006**, *74*, 054302. [CrossRef]
32. Cai, Q.Y. Eavesdropping on the two-way quantum communication protocols with invisible photons. *Phys. Lett. A* **2006**, *351*, 23–25. [CrossRef]
33. Deng, F.G.; Li, X.H.; Zhou, H.Y.; Zhang, Z.J. Improving the security of multiparty quantum secret sharing against Trojan horse attack. *Phys. Rev. A—At. Mol. Opt. Phys.* **2005**, *72*, 044302. [CrossRef]
34. Cabello, A. Quantum key distribution in the Holevo limit. *Phys. Rev. Lett.* **2000**, *85*, 5635. [CrossRef]
35. Feng, Y.H.; Zhou, R.G.; Zhang, X.X. Controlled bidirectional quantum secure direct communication with hyperentangled Bell states. *Phys. Scr.* **2025**, *100*, 025104. [CrossRef]
36. Zhou, R.G.; Zhang, X.X.; Li, F. Three-party semi-quantum protocol for deterministic secure quantum dialogue based on GHZ states. *Quantum Inf. Process.* **2021**, *20*, 153. [CrossRef]
37. Pan, H.M. Semi-Quantum Dialogue with Bell Entangled States. *Int. J. Theor. Phys.* **2020**, *59*, 1364–1371. [CrossRef]
38. Shi, G.F. Cryptanalysis and Improvement of Semi-Quantum Dialogue with Bell Entangled States. *Int. J. Theor. Phys.* **2023**, *62*, 224. [CrossRef]