

Three-party semi-quantum dialogue enhanced with Grover's algorithm based encoding and hypergraph access control

Rui Tao(陶瑞), Jin-Zhe Jiang(蒋晋喆), and Zhi-Hua Zhang(章志华)
Citation: Chin. Phys. B, 2026, 35 (**7**): 070306. DOI: 10.1088/1674-1056/ae7274
http://cpb.iphy.ac.cn; http://iopscience.iop.org/cpb

What follows is a list of articles you may be interested in

Measurement-device-independent quantum key distribution with entanglement-assisted linear Bell state measurement

Cheng Zhang(张诚), Cheng Liu(刘成), Jiawei Ying(应佳伟), Shipu Gu(顾世浦), Lan Zhou(周澜), Yin Ma(马寅), Kang Gao(高亢), Hai Wei(魏海), Kai Wen(文凯), and Yubo Sheng(盛宇波)
Chin. Phys. B, 2026, 35 (**4**): 040310. DOI: 10.1088/1674-1056/ae3605

Partial-measurement-enhanced high-dimensional superdense coding in amplitude damping channel with memory

Xing Xiao(肖兴), Zhipeng Yang(杨志鹏), Yan-Ling Li(李艳玲), Fangqing Tang(唐方清), and Tian-Xiang Lu(卢天祥)
Chin. Phys. B, 2026, 35 (**4**): 040301. DOI: 10.1088/1674-1056/ae27b4

Encoding converters for quantum communication networks

Hua-Xing Xu(许华醒), Shao-Hua Wang(王少华), Ya-Qi Song(宋雅琪), Ping Zhang(张平), and Chang-Lei Wang(王昌雷)
Chin. Phys. B, 2025, 34 (**5**): 050310. DOI: 10.1088/1674-1056/adcdeb

Multi-protocol quantum key distribution decoding chip

Chun-Xue Zhang(张春雪), Jian-Guang Li(李建光), Yue Wang(王玥), Wei Chen(陈巍), Jia-Shun Zhang(张家顺), and Jun-Ming An(安俊明)
Chin. Phys. B, 2025, 34 (**5**): 050303. DOI: 10.1088/1674-1056/adb686

Continuous-variable quantum secure direct communication based on *N*-APSK with Boltzmann-Maxwell distribution

Zheng-Wen Cao(曹正文), Yu-Jie Zhang(张昱洁), Geng Chai(柴庚), Zhang-Tao Liang(梁章韬), Xin-Lei Chen(陈欣蕾), Lei Wang(王磊), and Yu-Jie Wang(王禹杰)
Chin. Phys. B, 2025, 34 (**3**): 030303. DOI: 10.1088/1674-1056/ada549

Three-party semi-quantum dialogue enhanced with Grover's algorithm based encoding and hypergraph access control

Rui Tao(陶瑞), Jin-Zhe Jiang(蒋晋喆), and Zhi-Hua Zhang(章志华)†

School of Cyber Science and Engineering, Nanjing University of Science & Technology, Jiangyin 214400, *China*

(Received 3 February 2026; revised manuscript received 24 May 2026; accepted manuscript online 26 May 2026)

We introduce a new three-party semi-quantum dialogue (3P-SQD) protocol that combines GHZ-state-based semi-quantum communication, a Grover's algorithm-driven 2-bit encoding scheme, and hypergraph-based access control. In each round, the fully quantum participant Alice sends two bits, whereas the semi-quantum participants Bob and Charlie, restricted to semi-quantum operations such as measurements in the computational basis and reflection, each transmit one bit. The protocol incorporates probe state checking, Grover's algorithm-based encoding, and hypergraph-based authorization. It achieves information-theoretic security and controlled access, while preserving high message throughput and imposing no additional requirements on the semi-quantum users.

Keywords: semi-quantum dialogue, Grover's algorithm based encoding, hypergraph access structure, quantum communication

PACS: 03.67.–a, 03.67.Ac, 03.67.Hk

DOI: 10.1088/1674-1056/ae7274 **CSTR:** 32038.14.CPB.ae7274

1. Introduction

Quantum communication has become a cornerstone technology for achieving information-theoretic security in the quantum information era. The earliest protocols, most notably BB84[1] and E91,[2] established the framework for quantum key distribution (QKD),[3] a seminal development that allows two parties to share secret keys with security guaranteed at the information-theoretic level, and has been extended to the level of quantum communication networks.[4–6] As research has progressed, the field has broadened to include more general communication tasks. Quantum secure direct communication (QSDC)[7] has emerged as a key research direction. Building on this, Long and his collaborators have advanced QSDC toward practical, high-rate, and device-independent secure communication, by introducing one-step transmission schemes, measurement-device-independent architectures, and hybrid entanglement-plus-single-photon implementations tailored for large-scale network deployment.[8–12] Currently, quantum secret sharing (QSS)[13] has progressed from its original proposal to contemporary protocols that incorporate measurement-device-independent frameworks and versatile access structures, including hypergraph-based constructions, enabling scalable multi-user systems and fine-grained control over authorization.[14–17]

Most quantum communication protocols proposed in the early days are based on the assumption that communication participants possess full quantum capabilities, including multi-basis state preparation,[18] entanglement manipulation,[19] and quantum measurement,[20] which can be technologically demanding.[21] To relax these requirements, the concept of semi-quantum communication was introduced.[22] In the semi-quantum model, the quantum user Alice has access to a quantum channel which starts at her lab, travels out, and returns to her. The semi-quantum user Bob (also called a classical user) can access a portion of this channel. Thus, semi-quantum protocols operate over a two-way quantum channel where qubits, or other quantum carriers, travel first from the quantum user to the classical user, then return to the quantum user.[23] Boyer *et al.* in 2007 formalized the first semi-quantum key distribution (SQKD).[22] The SQKD protocols place a restriction on the classical user. More specifically, for every qubit received, Bob may choose one of the following five allowed operations:[23]

(1) **Measure** Perform a Z basis measurement on the incoming qubit.

(2) **Prepare** Prepare a state in the Z basis and transmit it to Alice over the reverse channel.

(3) **Measure and resend** Perform a Z basis measurement on the incoming qubit and then resend the result to Alice as a Z basis qubit, i.e., send $|0\rangle$ if the measurement result is 0 and $|1\rangle$ if it is 1. It is actually a combination of the measure and prepare operations.

(4) **Reflect** Reflect the qubit back to Alice undisturbed.

(5) **Permute** Reorder the qubits received (or a subset of qubits received) without otherwise disturbing them.

The first SQKD protocol proposed by Boyer *et al.* restricted the semi-quantum users to measure and resend or reflect operations.[22] Some typical SQKD protocols proposed in

†Corresponding author. E-mail: zhzhang@njust.edu.cn

© 2026 Chinese Physical Society and IOP Publishing Ltd. All rights, including for text and data mining, AI training, and similar technologies, are reserved.

later studies reduce the requirements on participants by letting classical users select different operations or by modifying the qubits prepared by the quantum user. For example, measure or reflect operations were selected in Ref. [24]. In Ref. [25], the quantum user Alice only needs to prepare qubits in the $|+\rangle$ states, compared to the four states of $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$ in Ref. [22].

SQKD inherits core security foundations from traditional QKD but evolves distinct characteristics tailored to its semi-quantum architecture. Both QKD and SQKD adhere to information-theoretic unconditional security,[1,22,26] and incorporate noise tolerance mechanisms.[27] However, critical differences emerge from SQKD's asymmetric user model: QKD requires both parties to possess full quantum capabilities like state preparation and measurement,[1] while SQKD restricts one user to classical operations,[22,24] leading to distinct robustness definitions. SQKD's robustness mandates that any eavesdropping attempt to gain information introduce detectable errors,[22] which addresses the limitations of classical users. Regarding critical security considerations, SQKD has been proven secure against coherent attacks through reductions to one-way quantum protocols and analyses of collective attacks.[28,29] The finite-key effect is explicitly addressed in practical SQKD research, with security proofs for mediated protocols incorporating device imperfections and finite-key analyses to ensure real-world applicability.[30] For eavesdropper assumptions, SQKD follows the same model as QKD, assuming an adversary bounded only by the laws of physics (computationally unbounded, capable of arbitrary quantum operations on the channel).[22,27] Collectively, these security characteristics position SQKD as a promising bridge between classical and quantum cryptography, retaining unconditional security while addressing practical deployment challenges.

The framework of SQKD was extended to two-party quantum dialogue[31–34] by Shukla *et al.* in 2017,[35] which is naturally called semi-quantum dialogue (SQD). Subsequent research on SQD sought to refine the existing fully quantum dialogue protocols by reducing the user's quantum capacity while maintaining security guarantees. Liu *et al.* designed a single-photon-based SQD architecture that removed the need for entanglement and complex quantum measurements.[36] Pan *et al.* strengthened protocol robustness by employing Bell state encoding and qubit reordering to counter intercept-resend and entanglement-measurement attacks without increasing user-side quantum requirements.[37] Within the two-party setting, SQD protocols ensure bidirectional information exchange through techniques such as channel-checking states, encoding on single-photon or entangled carriers, and error monitoring. However, additional optimizations, including throughput improvements based on Grover's algorithm-style quantum encoding[38,39] and single-photon implementations tailored for classically limited devices,[36] further enhance communication efficiency and practical deployability.

Building on these foundational developments, researchers extended semi-quantum dialogue beyond the traditional two-user setting to enable cooperative communication among multiple parties. Early work includes the three-step semi-quantum secure direct communication protocol introduced by Zou *et al.*,[40] followed by multi-party SQD schemes and GHZ-based variants that exploit multipartite entanglement to support larger groups of users.[41,42] The functionality of SQD was further broadened through mechanisms such as hypergraph-based access control,[15–17] supervisory control models,[43] and authenticated semi-quantum key distribution protocols,[44] which together enhanced both flexibility and security in practical use. However, these existing designs still suffer from inherent constraints, like limited communication capacity, insufficient support for coordinated interactions among multiple users, and susceptibility to participant impersonation, underscoring the need for a more powerful framework. These issues naturally lead to the study of three-party semi-quantum dialogue (3P-SQD), where preserving multipartite GHZ correlations over noisy channels and orchestrating joint security checks among semi-quantum users pose additional challenges. The protocol of Zhou *et al.*,[45] along with later improvements targeting higher transmission efficiency and stronger identity authentication,[43] constitutes an initial attempt to cope with these challenges. Yet, in the 3P-SQD setting, several practical requirements are still not fully satisfied: (i) enhancing the information rate per entangled state to ensure protocol efficiency in real-world networks; and (ii) enabling fine-grained and adaptable access control so that only designated subsets of participants can reconstruct shared secrets, while others are denied access.

The present study tries to meet these requirements by introducing a new 3P-SQD protocol that integrates GHZ state correlation, Grover's-algorithm-inspired 2-bit encoding to enhance throughput, and hypergraph-based access structures to enable flexible authorization. Two parties, Bob and Charlie, operate strictly in a semi-quantum manner, while the fully quantum user Alice is responsible for generating entanglement, performing measurements, and conducting security checks. The protocol provides higher efficiency and controlled information recovery ability restricted to authorized subsets of participants.

The remainder of this paper is organized as follows. In Section 2 we introduce the theoretical background, participant capabilities, quantum resources, and the hypergraph-based access model used in our setting. In Section 3 we detail the proposed three-party semi-quantum dialogue protocol and give an example to illustrate it. In Section 4 we present the pseudocode representation of the protocol. In Section 5 we analyze

the correctness of the protocol. In Section 6 we analyze the security from four aspects. In Section 7 we evaluate the complexity and efficiency of our protocol. Finally, we conclude the work and outline directions for future research in Section 8.

2. Preliminaries

2.1. Participants and semi-quantum roles

The proposed protocol involves three parties with heterogeneous quantum capabilities under the semi-quantum communication model. Firstly, Alice is a fully quantum-capable participant. She can prepare multipartite entangled states, including GHZ states and ancillary Grover registers, perform measurements in multiple bases (e.g., Z and X bases), and implement single- and two-qubit quantum gates. Alice is also responsible for inserting and detecting probe states.

We notice that some literature refers to the single-qubit states adopted in channel security detection as decoy states[42] or decoy photons.[45] To avoid confusion with the concept of "decoy states" in decoy-state QKD,[46–48] we adopt the term "probe states" in this paper, which denote additional single-qubit detection states inserted into transmission sequences exclusively for channel eavesdropping detection.

Secondly, Bob and Charlie are semi-quantum participants equipped with limited quantum functionality. Their operations are restricted to measuring incoming qubits in the computational (Z) basis, reflecting qubits without disturbance, and resending qubit sequences. This constrained operational model, as introduced in semi-quantum communication,[22] substantially reduces implementation complexity while preserving the quantum correlations required for secure interactive communication.

Finally, two types of communication channels are assumed. Quantum channels are used to transmit GHZ triplets, probe states, and Grover-encoded ancillary qubits. For the correctness and security analysis developed in this work, these channels are modeled as ideal noiseless channels. In practical implementations, however, channel attenuation, decoherence, detector dark counts, and imperfect optical alignment will introduce additional losses and errors. These implementation-related issues do not change the logical structure of the protocol, but they affect the achievable transmission distance, the effective detection probability, and the tolerable error threshold. An authenticated classical channel is employed for publishing measurement outcomes, parity information, and Grover decoding-related announcements, which prevents impersonation attacks and ensures the integrity of public communications.

2.2. Encoding and security resources

The quantum resources required in the protocol include:

(1) **Grover registers** To enhance information density, for the i-th GHZ state, Alice locally prepares a 2-qubit register in a uniform state

$$|S_i\rangle = \frac{1}{2}(|00\rangle + |01\rangle + |10\rangle + |11\rangle), \tag{1}$$

corresponding to the 2-bit message $w_{\mathrm{A},i} \in \{00, 01, 10, 11\}$. The target state $|w_{\mathrm{A},i}\rangle$ for Grover iteration is one of the four computational basis states $|w_{\mathrm{A},i}\rangle \in \{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$. Grover iterations amplify the amplitude of the target state starting from the superposition $|S_i\rangle$, enabling deterministic decoding by authorized participants.[38]

(2) **Grover iteration and amplification process** The Grover iteration consists of two unitary operators $U_{w_{\mathrm{A},i}} = I - 2|w_{\mathrm{A},i}\rangle\langle w_{\mathrm{A},i}|$ and $U_{S_i} = 2|S_i\rangle\langle S_i| - I$. The oracle $U_{w_{\mathrm{A},i}}$ flips the phase of the target state, and U_{S_i} performs reflection about the mean amplitude. For a 2-qubit space, one Grover iteration is sufficient to amplify the amplitude of the target basis state to unity. For instance, if $w_i = 10$, the oracle operation yields

$$U_{w_i}|x\rangle = \begin{cases} -|x\rangle, & x = 10, \\ |x\rangle, & x \neq 10, \end{cases} \tag{2}$$

resulting in the amplitude of $|10\rangle$ becoming -0.5 while others remain 0.5. The diffusion operator $U_S = 2|S\rangle\langle S| - I$ then reflects the state about the mean amplitude, raising the amplitude of $|10\rangle$ to approximately 1. Consequently, after a single iteration, the output state is $|w_i\rangle$, ensuring that Alice can deterministically encode each 2-bit message into the amplified state. The gate realization of the composite operator $U_{S_i}U_{w_{\mathrm{A},i}}$ is presented in Fig. 1.

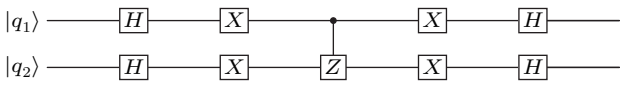


Fig. 1. Gate-level realization of the compositive operator $U_{S_i}U_{\omega_{\mathrm{A},i}}$ used in the Grover amplification stage. For the 2-qubit register, this circuit implements $U_{S_i} = 2|S_i\rangle\langle S_i| - I$ (up to a global phase), reflecting the current state about the mean amplitude of the uniform superposition. Combined with the oracle $U_{w_{\mathrm{A},i}}$, it completes one Grover iteration and deterministically amplifies the target basis state $|w_{\mathrm{A},i}\rangle$.

(3) **Probe states** In addition to the GHZ states for encoding, probe states are used only for channel-disturbance detection and are not used for message encoding. In the first checking round, Alice randomly prepares probe states selected from two mutually unbiased bases $\{|0\rangle, |1\rangle\}$ and $\{|+\rangle, |-\rangle\}$, and inserts them into the traveling sequences sent to Bob and Charlie. In the second checking round, Bob and Charlie, constrained by the semi-quantum model, randomly prepare fresh probe states only from the computational basis $\{|0\rangle, |1\rangle\}$. These second-round probe states are inserted into the returned sequences to check the integrity of the backward channels.

2.3. Hypergraph-based access structures

In classical secret sharing, an access structure defines which subsets of participants are authorized to reconstruct the

secret and which are not. Traditional access structures are typically represented by simple sets of authorized groups. However, as the number of participants and the relationships among them grow, simple pairwise or threshold structures become insufficient to describe complex multi-party authorization. To address this, the concept of a hypergraph is introduced, where each participant is represented as a vertex, and each hyperedge corresponds to an authorized subset of participants that can jointly reconstruct a secret.[15,16]

A hypergraph-based access structure (HBAS) in quantum communication generalizes classical secret sharing by mapping each quantum secret or message to one or more hyperedges instead of a single subset. This model enables flexible, hierarchical, and overlapping authorization relationships among multiple participants, making it suitable for quantum network environments involving multiple semi-quantum users. For example, in a three-party scenario with participants $\{\mathrm{A},\mathrm{B},\mathrm{C}\}$, possible hyperedges may include $\{\mathrm{A},\mathrm{B}\}$, $\{\mathrm{A},\mathrm{C}\}$, and $\{\mathrm{A},\mathrm{B},\mathrm{C}\}$, representing different authorized coalitions. Each hyperedge defines an independent access rule for reconstructing a particular secret.

In this protocol, we adopt the HBAS framework[17] to manage access control for each 2-bit message encoded by the fully quantum participant (Alice). Each message corresponds to a specific hyperedge that determines which semi-quantum participants are required for its recovery. Only members of the corresponding hyperedge can combine their classical measurement results with Alice's public announcements to recover the message, while any unauthorized subsets, even if they collude, cannot obtain complete information about the secret. This property provides both confidentiality and fine-grained access control in the semi-quantum setting.

2.4. Hypergraph-based access control

Following the HBAS framework, each encoded secret or 2-bit message in the proposed protocol is assigned to one authorized subset of participants (hyperedge). For the three-party case, the set of possible authorized coalitions is

$$\mathcal{H} = \{\{\mathrm{A},\mathrm{B}\},\{\mathrm{A},\mathrm{C}\},\{\mathrm{A},\mathrm{B},\mathrm{C}\}\}. \tag{3}$$

Each $\mathcal{H}_j \in \mathcal{H}$ defines which subset can reconstruct the message. The access control operates as follows:

(1) **Authorized access** Participants belonging to a hyperedge $\mathcal{H}_j$ can jointly reconstruct the secret or 2-bit message by combining their classical shares and Alice's public announcements. For example, if $\mathcal{H}_j = \{\mathrm{A},\mathrm{B}\}$, only Alice and Bob together can recover the message.

(2) **Unauthorized restrictions** Any subset $\mathcal{U} \notin \mathcal{H}$ lacks sufficient information to determine the secret, as missing classical shares or Grover-encoded data renders reconstruction impossible. For instance, Bob or Charlie alone cannot deduce the message without Alice's measurement outcomes.

(3) **Flexible control** HBAS provides hierarchical flexibility, allowing the protocol designer to assign different hyperedges to different messages. Thus, one message may require cooperation between Alice and Bob, while another may require all three participants, reflecting distinct authorization levels.

(4) **Integration with semi-quantum dialogue** The HBAS mechanism naturally integrates with the GHZ-based semi-quantum dialogue and enforces access control without increasing the quantum capability requirements for semi-quantum users, since authorization is achieved purely through classical correlations and the structure of hyperedges. Figure 2 illustrates the hypergraph-based access structure for the three-party semi-quantum dialogue. In this figure, each node denotes a participant in the protocol, while each ellipse represents an authorized hyperedge associated with a specific secret message. The symbols w_i, w_j, and w_k denote different 2-bit messages encoded by the fully quantum participant, each of which is assigned to a particular hyperedge. The hyperedge labeled $\{\mathrm{A},\mathrm{B},\mathrm{C}\}$ corresponds to full cooperation among all three parties, whereas the hyperedges $\{\mathrm{A},\mathrm{B}\}$ and $\{\mathrm{A},\mathrm{C}\}$ represent partial authorized coalitions. Only participants belonging to the same hyperedge can jointly reconstruct the corresponding message, while any unauthorized subset is unable to recover the secret.

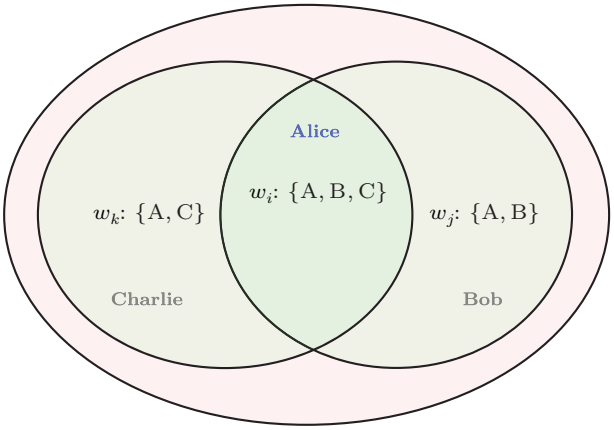


Fig. 2. Hypergraph-based access structure for the three-party semi-quantum dialogue.

In the present three-party setting, the adopted HBAS is not introduced to increase the quantum capability requirements, but to provide an authorization model that cannot be expressed conveniently by simpler threshold-type rules. For example, the authorized family $\mathcal{H} = \{\{\mathrm{A},\mathrm{B}\},\{\mathrm{A},\mathrm{C}\},\{\mathrm{A},\mathrm{B},\mathrm{C}\}\}$ allows Alice to collaborate either with Bob or with Charlie, while excluding Bob–Charlie-only recovery. Such overlapping but non-symmetric coalitions are difficult to represent by a single threshold policy. A 2-out-of-3 threshold rule would also authorize $\{\mathrm{B},\mathrm{C}\}$, which is not desired here. Likewise, tree-based access structures are more suitable for hierarchical

authorization, but are less natural for the present overlapping-coalition setting. Therefore, HBAS provides a more direct and flexible representation of the intended access policy in this protocol.

2.5. Security considerations

Before protocol execution, the following security assumptions and considerations are made:

(1) **Quantum channel security** The GHZ states provide the multipartite correlations required for dialogue and message recovery, while the probe states serve as independent checking states for the traveling sequences. Because the protocol involves two-way transmission between Alice and the semi-quantum participants, explicit probe checking is used to detect eavesdropping and channel disturbance. If the observed error rate exceeds the preset threshold, the protocol is aborted.

(2) **Semi-quantum participant compliance** Semi-quantum participants (Bob and Charlie) are assumed to follow the prescribed operations faithfully, namely, prepare a state in the computational basis, measure in the computational basis and resend, and reflect, hereafter abbreviated as M/R operations. Any deviation, whether intentional or caused by device imperfections, can be detected by Alice through the consistency of the GHZ correlations.

(3) **Classical channel authentication** All classical channels used for publishing measurement outcomes, parity information, or Grover decoding hints are authenticated. This prevents impersonation attacks and ensures integrity of the announced data.

(4) **Probe state checking** Randomly interleaved probe states are used to test whether the traveling sequences have been disturbed during transmission. In the first checking round, Alice prepares probe states selected from the set $\{|0\rangle,|1\rangle,|+\rangle,|-\rangle\}$. In the second checking round, Bob and Charlie prepare probe states from the Z basis $\{|0\rangle,|1\rangle\}$, which is consistent with their semi-quantum capability restrictions and is used to check the backward channels after message encoding.

3. Protocol description

3.1. Phase I: Preparation and first probe detection

In the first phase, the participants accomplish the preparation of GHZ states, particle distribution, and security detection of forward channels. The details are as follows:

(1) **GHZ state preparation** Alice prepares N GHZ states and partitions the qubits into three ordered sequences $S_{\mathrm{A}} = [P_1(\mathrm{A}),P_2(\mathrm{A}),\ldots,P_N(\mathrm{A})]$, $S_{\mathrm{B}} = [P_1(\mathrm{B}),P_2(\mathrm{B}),\ldots,P_N(\mathrm{B})]$ and $S_{\mathrm{C}} = [P_1(\mathrm{C}),P_2(\mathrm{C}),\ldots,P_N(\mathrm{C})]$, where $P_i(\mathrm{A})$, $P_i(\mathrm{B})$, and $P_i(\mathrm{C})$ denote the first, second, and third qubits of the ith GHZ state, respectively.

(2) **First-round probe states insertion** To check the forward quantum channels, Alice randomly prepares $2n_1$ probe states selected from $\{|0\rangle,|1\rangle,|+\rangle,|-\rangle\}$. She inserts n_1 probe states into S_{B} and another n_1 into S_{C}, and records their positions, preparation bases, and initial states. For simplicity and for comparison with existing GHZ-based three-party SQD protocols, we take $n_1 = N$ in this work.

(3) **Transmission and semi-quantum operations on first-round probes** Alice sends the probe-interleaved sequences to Bob and Charlie. After Bob and Charlie confirm receipt, Alice announces the positions of the probe states. Bob and Charlie perform one of the following semi-quantum operations on the received probe states: (a) **Reflect**: reflect the qubit back to Alice without disturbance; or (b) **Measure and resend**: measure the qubit in the computational (Z) basis and resend the corresponding Z-basis state. After Alice receives the returned probe states, Bob and Charlie announce their chosen operations.

(4) **First probe-state checking** After receiving the returned probe states, Alice checks them according to their preparation bases and the operations announced by Bob and Charlie. For a reflected probe state, Alice measures it in the same basis as the preparation basis and compares the result with the initial state. For a measure-and-resend probe state, Alice measures the returned qubit in the Z basis and compares her outcome with the measurement result announced by the corresponding semi-quantum participant. Alice then computes

$$\varepsilon_1 = \frac{\text{Number of inconsistent first-round probe outcomes}}{\text{Total number of checked first-round probe states}}. \quad (4)$$

If $\varepsilon_1 > \varepsilon_{\mathrm{th}}$, the protocol is aborted. Otherwise, the protocol proceeds to the message-encoding phase.

3.2. Phase II: Semi-quantum message encoding and second probe detection

In the second phase, the semi-quantum participants complete information encoding, and all participants jointly conduct security detection of the backward channels. The details are as follows:

(1) **Semi-quantum message encoding** After passing the first probe check, Bob and Charlie encode the secret bits $m_{\mathrm{B},i}$ and $m_{\mathrm{C},i}$ on the positions of $P_i(\mathrm{B})$ and $P_i(\mathrm{C})$, respectively. The encoding operation follows the corresponding relationship below:

$$0 \rightarrow \text{Reflect (R)}, \quad 1 \rightarrow \text{Measure–Flip-Resend (M-flip)}. \quad (5)$$

Specifically, to encode bit 1, the participant measures the qubit in the computational (Z) basis, obtains $r \in \{0,1\}$, flips the result, and resends the opposite computational-basis state; to encode bit 0, the qubit is simply reflected. The local measurement outcomes are recorded for later message recovery.

(2) **Second-round probe state insertion** To detect eavesdropping on the backward quantum channels, Bob and Charlie each randomly prepare n_2 fresh probe states selected from the computational basis $\{|0\rangle,|1\rangle\}$. They randomly insert these probe states into S_B and S_C and record the corresponding probe positions and initial states. The resulting sequences are denoted by S'_B and S'_C, respectively. Bob and Charlie send S'_B and S'_C back to Alice. For simplicity, we take $n_2 = N$ in this work.

(3) **Second probe-state checking** After Alice confirms that she has received S'_B and S'_C, Bob and Charlie announce the positions and initial states of their second-round probe states. Alice measures these probe states in the computational basis and compares her measurement outcomes with the announced initial states. She then computes

$$\varepsilon_2 = \frac{\text{Number of inconsistent second-round probe outcomes}}{\text{Total number of checked second-round probe states}}. \tag{6}$$

If $\varepsilon_2 > \varepsilon_{\text{th}}$, the protocol is aborted. Otherwise, Alice removes the second-round probe states and accepts the remaining carrier states for the subsequent recovery stage.

(4) **Message correlation assurance** Due to the intrinsic GHZ correlations, Alice can infer Bob and Charlie's encoded bits from her measurements, even though Bob and Charlie perform only limited semi-quantum operations.

3.3. Phase III: Grover-state encoding with hypergraph-controlled masking

After the second probe detection is successfully passed, Alice proceeds to encode her own 2-bit message in a quantum form using a Grover register, while the GHZ correlations are exploited to enforce hypergraph-based access control.

(1) **GHZ measurement and correlation extraction** Alice measures her GHZ qubit in the computational basis and records the triplet $(r_{A,i}, r_{B,i}, r_{C,i}) \in \{0,1\}^3$, where $r_{B,i}$ and $r_{C,i}$ are inferred from the returned sequences and GHZ correlations.

(2) **Grover state preparation** Alice selects a 2-bit message $w_{A,i} \in \{00,01,10,11\}$, prepares a 2-qubit Grover register $|S_i\rangle$ in Eq. (1), applies one Grover iteration and obtains $|\psi_i\rangle = U_{S_i} U_{w_{A,i}} |S_i\rangle = |w_{A,i}\rangle$, where $|w_{A,i}\rangle$ is one of $\{|00\rangle,|01\rangle,|10\rangle,|11\rangle\}$ corresponding to Alice's 2-bit message.

(3) **Hypergraph-controlled masking operation** Let $\mathcal{H}_j \subseteq \{A,B,C\}$ denote the authorized hyperedge for the i-th round. Alice applies a controlled phase operation $U_{\mathcal{H}_j} = Z^{f_{\mathcal{H}_j}(r_{B,i}, r_{C,i})}$, on the Grover register, where Z is the Pauli-Z operator acting on the Grover register. The control function $f_{\mathcal{H}_j}$ is defined as

$$f_{\mathcal{H}_j}(r_{B,i}, r_{C,i}) = \begin{cases} r_{B,i}, & \mathcal{H}_j = \{A,B\}, \\ r_{C,i}, & \mathcal{H}_j = \{A,C\}, \\ r_{B,i} \oplus r_{C,i}, & \mathcal{H}_j = \{A,B,C\}. \end{cases} \tag{7}$$

This operation masks the Grover state in a manner that can only be inverted by members of the authorized hyperedge.

(4) **Public announcement** Alice publicly announces the GHZ type used in the i-th round, the hyperedge label $\mathcal{H}_j$ and the Grover decoding rule (i.e., the functional form of $f_{\mathcal{H}_j}$), but does not reveal the values of $r_{B,i}$ or $r_{C,i}$.

3.4. Phase IV: Local message recovery

In the final phase, the three participants recover the secret information sent by others based on the hypergraph structure and their respective authorities. The specific details are as follows:

(1) **Recovery by authorized semi-quantum participants** Consider an authorized participant $U \in \mathcal{H}_j$. Using their locally obtained measurement outcome (e.g., $r_{B,i}$ for Bob or $r_{C,i}$ for Charlie), participant U evaluates the control function $f_{\mathcal{H}_j}(r_{B,i}, r_{C,i})$ and applies the corresponding inverse phase correction to the Grover register. The participant then measures the Grover register in the computational basis and deterministically obtains $w_{A,i}$. This recovery is entirely local and does not require assistance from unauthorized parties.

(2) **Failure of unauthorized participants** Any participant $U \notin \mathcal{H}_j$ lacks sufficient classical information to determine $f_{\mathcal{H}_j}(r_{B,i}, r_{C,i})$. As a result, the reduced density matrix of the Grover register from their perspective is

$$\rho_U = \frac{1}{2}\Big(|w_{A,i}\rangle\langle w_{A,i}| + Z|w_{A,i}\rangle\langle w_{A,i}|Z\Big), \tag{8}$$

which yields a uniform outcome distribution over the computational basis. Hence, the message $w_{A,i}$ is information-theoretically unrecoverable by any unauthorized subset.

(3) **Recovery of semi-quantum messages by Alice** Using her own measurement outcome $r_{A,i}$ and the GHZ correlations, Alice deterministically infers the classical messages $m_{B,i}$ and $m_{C,i}$ encoded by Bob and Charlie via the M/R operations.

3.5. Illustrative example

To illustrate the protocol workflow, consider two consecutive GHZ rounds, both using the standard tripartite entangled state

$$|\text{GHZ}\rangle = \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle), \tag{9}$$

shared among Alice (A), Bob (B), and Charlie (C). The first round corresponds to a full-access hyperedge $\mathcal{H}_1 = \{A,B,C\}$, while the second round involves a restricted hyperedge $\mathcal{H}_2 =$

$\{A,B\}$, meaning only Alice and Bob are authorized to recover the secret message in that round. We illustrate the SQD process in the following four steps.

Step 1: GHZ state preparation and first probe detection Alice prepares the GHZ state in Eq. (9) and interleaves first-round probe states randomly chosen from $\{|0\rangle,|1\rangle,|+\rangle,|-\rangle\}$ into S_B and S_C before transmission. Bob and Charlie each perform random M or R operations on the sampled probe states and return the sequences. For the reflected probe states, Alice measures them in their preparation bases; for the measure-and-resend probe states, Alice measures them in the Z basis and compares her outcomes with Bob's or Charlie's announced measurement results. Alice then computes the first-stage error rate ε_1.

Step 2: Semi-quantum message encoding by Bob and Charlie Bob encodes $m_{B,1}=1$ using the M-flip operation, i.e., he measures the received qubit in the Z basis, obtains outcome r_B, flips it ($0\leftrightarrow 1$), and resends the qubit. Charlie encodes $m_{C,1}=0$ by performing the reflection (R) operation without measurement. After the message encoding operation, Bob and Charlie each randomly prepare second-round probe states from the computational basis $\{|0\rangle,|1\rangle\}$ and insert them into their returned sequences. Alice performs operations of second probe-state checking, which are described in the phase II. She computes the second-stage error rate ε_2. If $\varepsilon_2\le\varepsilon_{th}$, the returned carrier qubits are accepted for the subsequent Grover-state encoding and message-recovery stage; otherwise, the communication is aborted.

Step 3: Grover encoding and message recovery under full access Alice encodes her 2-bit message $w_{A,1}=10$ by applying one Grover iteration $|\psi_1\rangle=U_{S_1}U_{w_{A,1}}|S_1\rangle$ with $|S_1\rangle=(|00\rangle+|01\rangle+|10\rangle+|11\rangle)/2$. Suppose Alice's measurement result on the GHZ state is $(r_{A,1},r_{B,1},r_{C,1})=(0,1,0)$. The parity and key are computed as

$$\begin{aligned}P_1&=r_{A,1}\oplus r_{B,1}\oplus r_{C,1}=1,\\ K_1&=(r_{A,1},r_{B,1}\oplus r_{C,1})=(0,1).\end{aligned}\tag{10}$$

Alice publishes $C_1=w_{A,1}\oplus K_1=10\oplus 01=11$. Since $\mathcal{H}_1=\{A,B,C\}$, all three participants can jointly reconstruct $w_{A,1}=10$.

Step 4: Restricted hyperedge and selective access In the next step, the authorized subset is $\mathcal{H}_2=\{A,B\}$, while Charlie is excluded from message recovery. Alice again prepares the GHZ state in Eq. (9), inserts probe states, and verifies $\varepsilon_1\le\varepsilon_{th}$. Bob encodes $m_{B,2}=0$ by reflecting the qubit (R), whereas Charlie performs normal reflection without being authorized to recover the message. Alice's 2-bit message for this step is $w_{A,2}=01$. Assume Alice's measurement result is $(r_{A,2},r_{B,2},r_{C,2})=(1,1,1)$; she computes

$$\begin{aligned}P_2&=r_{A,2}\oplus r_{B,2}\oplus r_{C,2}=1,\\ K_2&=(r_{A,2},r_{B,2}\oplus r_{C,2})=(1,0),\end{aligned}\tag{11}$$

and publishes $C_2=w_{A,2}\oplus K_2=01\oplus 10=11$. Only Alice and Bob can jointly compute

$$w_{A,2}=C_2\oplus K_2=11\oplus 10=01,\tag{12}$$

whereas Charlie alone cannot recover $w_{A,2}$ due to insufficient classical information.

For concreteness, Tables 1 and 2 are presented to enumerate all message-recovery cases under the three authorized hyperedges $\{A,B\}$, $\{A,C\}$, and $\{A,B,C\}$, respectively, for the initial state $(|000\rangle+|111\rangle)/\sqrt{2}$. For the hyperedges $\{A,B\}$ and $\{A,C\}$, the number of cases is $4\times 2=8$, since Alice contributes a 2-bit message and only one semi-quantum participant is involved in the authorized recovery. For the hyperedge $\{A,B,C\}$, the number of cases is $4\times 2\times 2=16$, since both Bob and Charlie participate in the authorized recovery.

Table 1. Complete recovery cases for the authorized hyperedge $\{A,B\}$ and $\{A,C\}$ under initial state $|\Psi\rangle_{ABC}=\frac{1}{\sqrt{2}}(|000\rangle+|111\rangle)_{ABC}$, where ARR is abbreviation of authorized recovery result.

Case	$w_{A,i}$	$m_{B,i}$	$m_{C,i}$	ARR	Case	$w_{A,i}$	$m_{B,i}$	$m_{C,i}$	ARR
1	00	0	–	$\{A,B\}\to 00$	1	00	–	0	$\{A,C\}\to 00$
2	00	1	–	$\{A,B\}\to 00$	2	00	–	1	$\{A,C\}\to 00$
3	01	0	–	$\{A,B\}\to 01$	3	01	–	0	$\{A,C\}\to 01$
4	01	1	–	$\{A,B\}\to 01$	4	01	–	1	$\{A,C\}\to 01$
5	10	0	–	$\{A,B\}\to 10$	5	10	–	0	$\{A,C\}\to 10$
6	10	1	–	$\{A,B\}\to 10$	6	10	–	1	$\{A,C\}\to 10$
7	11	0	–	$\{A,B\}\to 11$	7	11	–	0	$\{A,C\}\to 11$
8	11	1	–	$\{A,B\}\to 11$	8	11	–	1	$\{A,C\}\to 11$

Table 2. Complete recovery cases for the authorized hyperedge $\{A,B,C\}$ under the initial state $|\Psi\rangle_{ABC}=\frac{1}{\sqrt{2}}(|000\rangle+|111\rangle)_{ABC}$, where ARR is abbreviation of authorized recovery result.

Case	$w_{A,i}$	$m_{B,i}$	$m_{C,i}$	ARR	Case	$w_{A,i}$	$m_{B,i}$	$m_{C,i}$	ARR
1	00	0	0	$\{A,B,C\}\to 00$	9	10	0	0	$\{A,B,C\}\to 10$
2	00	0	1	$\{A,B,C\}\to 00$	10	10	0	1	$\{A,B,C\}\to 10$
3	00	1	0	$\{A,B,C\}\to 00$	11	10	1	0	$\{A,B,C\}\to 10$
4	00	1	1	$\{A,B,C\}\to 00$	12	10	1	1	$\{A,B,C\}\to 10$
5	01	0	0	$\{A,B,C\}\to 01$	13	11	0	0	$\{A,B,C\}\to 11$
6	01	0	1	$\{A,B,C\}\to 01$	14	11	0	1	$\{A,B,C\}\to 11$
7	01	1	0	$\{A,B,C\}\to 01$	15	11	1	0	$\{A,B,C\}\to 11$
8	01	1	1	$\{A,B,C\}\to 01$	16	11	1	1	$\{A,B,C\}\to 11$

4. Algorithm: Pseudocode representation

Algorithm 1 Three-party semi-quantum dialogue with Grover's algorithm based encoding.

Input: Alice's messages $\{w_{A,i}\}_{i=1}^N$ (each $w_{A,i}$ is a 2-bit message encoded via Grover iteration), Bob's messages $\{m_{B,i}\}_{i=1}^N$, Charlie's messages $\{m_{C,i}\}_{i=1}^N$.

Output: Recovered messages at all parties.

1: **for** $i=1$ to N **do**

2: Alice prepares $|GHZ_i\rangle$, inserts first-round probe states randomly chosen from $\{|0\rangle,|1\rangle,|+\rangle,|-\rangle\}$ into S_B and S_C, and sends the sequences to Bob and Charlie

3: Bob/Charlie perform Reflect or Measure-and-Resend operations on the first-round probe states

Algorithm 1 Continued.

4: Alice checks reflected probes in their preparation bases and Measure-and-Resend probes in the Z basis, calculates ε_1, and terminates if $\varepsilon_1 > \varepsilon_{\text{th}}$
5: Bob/Charlie encode their classical message bits on the remaining carrier qubits, insert second-round fresh Z-basis probe states chosen from $\{|0\rangle, |1\rangle\}$, and return the updated sequences to Alice
6: After Alice confirms receipt, Bob/Charlie announce the positions and initial states of the second-round probe states; Alice measures them in the Z basis, calculates ε_2, and terminates if $\varepsilon_2 > \varepsilon_{\text{th}}$
7: Alice applies the Grover iteration $|\psi_i\rangle = U_{S_i} U_{w_{\text{A},i}} |S_i\rangle$ on her 2-qubit register, where $w_{\text{A},i}$ denotes her 2-bit message (b_{i1}, b_{i2})
8: Alice measures the GHZ qubits, computes the parity P_i, constructs the key K_i, and publishes $C_i = w_{\text{A},i} \oplus K_i$ together with P_i and the GHZ type
9: Alice recovers $m_{\text{B},i}$ and $m_{\text{C},i}$; Bob/Charlie recover $w_{\text{A},i}$ from the Grover-encoded state and the published information
10: **end for**

5. Correctness analysis

The correctness of the protocol ensures that all legitimate parties can recover each other's messages with probability 1 in the absence of eavesdropping or channel noise.

5.1. GHZ correlation consistency

For each round, Alice prepares one of the eight standard tripartite GHZ basis states, which can be labeled by a three-bit string $(x, y, z) \in \{0,1\}^3$ as

$$|\text{GHZ}^{\pm}_{xyz}\rangle = \frac{1}{\sqrt{2}}\big(|xyz\rangle \pm |\bar{x}\bar{y}\bar{z}\rangle\big), \tag{13}$$

where $\bar{x} = x \oplus 1$, $\bar{y} = y \oplus 1$ and $\bar{z} = z \oplus 1$. The three-bit string (x, y, z) corresponds to $|\text{GHZ}^{+}_{xyz}\rangle$ and $(\bar{x}, \bar{y}, \bar{z})$ to $|\text{GHZ}^{-}_{xyz}\rangle$.

When Alice, Bob and Charlie measure their respective qubits on the computational basis, the measurement outcome $(r_{\text{A},i}, r_{\text{B},i}, r_{\text{C},i}) \in \{0,1\}^3$ must be one of the two classical bit strings (x, y, z) or $(\bar{x}, \bar{y}, \bar{z})$, as determined by the intrinsic correlations of the GHZ state.

Importantly, for both possible outcomes, the following correlation identities hold:

$$r_{\text{B},i} \oplus r_{\text{C},i} = y \oplus z, \tag{14}$$

$$r_{\text{A},i} \oplus r_{\text{B},i} \oplus r_{\text{C},i} = x \oplus y \oplus z. \tag{15}$$

These relations depend only on the GHZ label (x, y, z) and are independent of which computational basis component is obtained in the measurement.

As a result, Alice can deterministically infer the combined parity information of Bob and Charlie using the publicly known GHZ label. This enables the construction of the round key $K_i = (r_{\text{A},i},\ r_{\text{B},i} \oplus r_{\text{C},i})$, which is uniquely determined by the GHZ correlations and the local measurement outcomes.

Consequently, the parity consistency and key construction in each round are guaranteed by the structure of the GHZ basis itself, without requiring any additional hidden variables or collapse indicators.

5.2. Grover encoding determinism

For a two-qubit register, a single Grover iteration satisfies $|\psi_i\rangle = U_{S_i} U_{w_{\text{A},i}} |S_i\rangle = |w_{\text{A},i}\rangle$, so Alice's two-bit symbol is encoded deterministically in each round. As shown in the preliminary analysis in Subsection 2.2, a single iteration in a two-qubit system amplifies the target amplitude to 1, yielding the deterministic output state $|\psi_i\rangle = |w_i\rangle$. This ensures that Alice's Grover-encoded two-bit message can be recovered by authorized participants with high probability while preserving perfect distinguishability among the four message states.

5.3. Semi-quantum message recovery

Bob and Charlie recover Alice's 2-bit message using $w_i = C_i \oplus K_i = C_i \oplus (r_{\text{A},i},\ r_{\text{B},i} \oplus r_{\text{C},i})$. Given their own measurement outcomes $(r_{\text{B},i}, r_{\text{C},i})$, Bob and Charlie can reconstruct $K_i = (r_{\text{A},i}, r_{\text{B},i} \oplus r_{\text{C},i})$ and thus compute w_i deterministically. The GHZ correlations ensure that these values are consistent across all parties.

5.4. Hypergraph access control correctness

For a secret associated with an authorized subset $\mathcal{H}_j$, recovery requires

$$\mathcal{H}_j \subseteq \{\text{parties combining their classical shares}\}. \tag{16}$$

Only an authorized subset $\mathcal{H}_j$ (i.e., a set that contains all members required by the access structure) can reconstruct the secret. Any subset $\mathcal{U}$ that does not contain $\mathcal{H}_j$ (equivalently $\mathcal{H}_j \not\subseteq \mathcal{U}$) cannot recover the key, i.e., $\mathcal{H}_j \not\subseteq \mathcal{U}$ implies $K_i^{\mathcal{U}} \neq K_i$, and thus w_i remains unrecoverable by $\mathcal{U}$, i.e., $K_i^{\mathcal{U}} \neq K_i$ implies $w_i^{\mathcal{U}}$ is indeterminate.

6. Security analysis

6.1. Information-theoretic security

An external eavesdropper Eve only observes the public announcement $(C_i, P_i, \text{GHZ type})$. Without access to $(r_{\text{A},i}, r_{\text{B},i}, r_{\text{C},i})$, the 2-bit message w_i is perfectly masked by the one-time pad K_i; therefore, we have $H(w_i \mid C_i) = H(w_i)$, where H is the Shannon entropy, implying information-theoretic security. This means that knowing the ciphertext C_i provides no information about the secret w_i, i.e., the eavesdropper's uncertainty about w_i remains maximal.

6.2. Intercept-resend attack

For the first checking round, the probe states are randomly chosen from $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$. If Eve measures and resends a probe state in a randomly chosen basis, then any basis mismatch may disturb the returned state and can be detected by

Alice. In particular, for reflected probe states, Alice measures the returned qubit in the original preparation basis, so an intercept-measure-resend operation in the wrong basis introduces a nonzero error probability. For measure-and-resend probe states, Alice checks the consistency between her Z-basis measurement outcome and the semi-quantum user's announced Z-basis result. Therefore, as the number of checked probes increases, the probability that Eve remains undetected decreases exponentially.

For the second checking round, the probe states are restricted to $\{|0\rangle, |1\rangle\}$, because Bob and Charlie are semi-quantum users. This round mainly checks the integrity of the backward channels against replacement, tampering, and bit-flip disturbances on the returned sequences.

6.3. Entanglement-measurement attack

The entanglement-measurement attack in this paper can be analyzed by adopting the method in Ref. [45]. We assume that an eavesdropper Eve employs the same entanglement attack strategy in both the forward and backward channels. Eve entangles her auxiliary qubits with the transmitted quantum states, and intends to steal secret information by measuring her own auxiliary qubits without being detected by the eavesdropping check. According to Ref. [45], if Eve attempts to evade the two rounds of eavesdropping detection and obtain confidential information, her entangling operation will inevitably cause measurement deviations of Alice in the X basis or the Z basis. Such deviations can be counted and identified during the two eavesdropping detection processes. Therefore, the proposed scheme can effectively resist the entanglement-measurement attack.

6.4. Impersonation attack

Eve, attempting to impersonate Bob or Charlie, cannot generate the correct classical shares without knowledge of the GHZ initial states and local measurement results. Hypergraph access control further restricts secret reconstruction to authorized subsets only.

Overall, the proposed protocol simultaneously achieves confidentiality, integrity, authentication, and effective eavesdropping detection. Alice's 2-bit messages are perfectly protected by the one-time pad key K_i, ensuring information-theoretic confidentiality. Any attempt by an external eavesdropper or a dishonest participant to modify or inject quantum states is detected with high probability through the two rounds of probe state checking verification. Moreover, the intrinsic correlations of the GHZ states, together with the hypergraph-based access structure, prevent impersonation attacks and unauthorized message recovery. Consequently, the protocol provides a comprehensive level of security against standard quantum attacks in the semi-quantum setting.

7. Complexity and efficiency

This section evaluates the proposed three-party semi-quantum dialogue protocol from three aspects: information throughput, quantum-operation cost, and probe-state overhead. Finally, we compare our protocol with some recent three-party semi-quantum protocols.

7.1. Information throughput

In each effective GHZ round, Alice encodes a 2-bit message $w_{\mathrm{A},i} \in \{00, 01, 10, 11\}$ through the Grover-based register, while Bob and Charlie each contribute one classical bit, denoted by $m_{\mathrm{B},i} \in \{0, 1\}$ and $m_{\mathrm{C},i} \in \{0, 1\}$, respectively. Hence, the total amount of information associated with one GHZ group is $T_{\mathrm{GHZ}} = 2 + 1 + 1 = 4$ bits. Accordingly, for N GHZ groups, the cumulative throughput is $T_{\mathrm{total}} = 4N$ bits.

For comparison, in the three-party semi-quantum dialogue protocol of Zhou *et al.*,[45] the quantum participant contributes one bit per GHZ round, and each semi-quantum participant also contributes one bit, so the total throughput is $3N$ bits for N GHZ rounds. In the present protocol, the Grover-based encoding increases Alice's contribution from one bit to two bits, while the contributions of Bob and Charlie remain unchanged. As a result, the total throughput increases from $3N$ to $4N$ bits, giving a relative gain of

$$\eta_{\mathrm{gain}} = \frac{4N - 3N}{3N} = \frac{1}{3} \approx 33.3\%. \tag{17}$$

7.2. Quantum operation cost

The additional quantum cost introduced in the present scheme mainly arises from Alice's Grover-based encoding procedure. Since the Grover register contains two qubits, the search space consists of four computational basis states. In this case, a single Grover iteration is sufficient to drive the register to the target basis state corresponding to Alice's 2-bit message. Therefore, the encoding cost on Alice's side remains constant per round and can be written as $O\left(\sqrt{|S|}\right) = O(2) = O(1)$, where $|S| = 2^2 = 4$ is the size of the search space.

By contrast, Bob and Charlie still perform only the standard semi-quantum operations, namely, measurement in the Z basis, resend, and reflection. Thus, their operational cost remains constant for each traveling qubit, namely, $O_{\mathrm{semi}} = O(1)$.

7.3. Probe-state overhead

Let n_1 denote the number of first-round probe states inserted into each forward traveling sequence, and n_2 denote the number of second-round probe states inserted into each returned sequence. In the first checking round, Alice prepares n_1 probe states for the Alice–Bob channel and n_1 probe states for the Alice–Charlie channel, where the probe states are randomly chosen from $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$. In the second checking round, Bob and Charlie each prepare n_2 fresh Z-basis probe states from $\{|0\rangle, |1\rangle\}$. Thus, the total number of

probe states is $N_{\text{probe}} = 2n_1 + 2n_2$. For simplicity, we take $n_1 = n_2 = N$, and hence $N_{\text{probe}} = 4N$.

7.4. HBAS complexity and structural overhead

Besides improving authorization flexibility, the use of HBAS introduces an additional structural overhead that should be discussed explicitly. In the present three-party protocol, however, this overhead remains modest.

First, the HBAS mechanism does not add any extra quantum operations for the semi-quantum users. Bob and Charlie still perform only computational basis measurement, reflection, and sequence resending. The hypergraph policy affects only Alice's classical selection of the authorized hyperedge H_j and the corresponding masking rule $f_{H_j}(r_{\mathrm{B},i}, r_{\mathrm{C},i}) \in \{r_{\mathrm{B},i}, r_{\mathrm{C},i}, r_{\mathrm{B},i} \oplus r_{\mathrm{C},i}\}$, which requires only a constant-size classical computation in the three-party case.

Second, the additional communication overhead caused by HBAS is also limited in the present setting. For each round, Alice only needs to publish the label of the selected hyperedge together with the corresponding decoding rule. Since the number of admissible hyperedges is $|\mathcal{H}| = 3$, this policy overhead is $O(1)$ per round and is negligible compared with the quantum transmission cost.

Third, from a structural viewpoint, the complexity of HBAS grows with the number of authorized hyperedges. For a general n-party extension, if the access family contains $|\mathcal{H}|$ authorized hyperedges, then the policy-description cost scales as $O(|\mathcal{H}|)$, and the classical coordination cost for a round is related to the size of the selected authorized subset. Therefore, HBAS provides higher expressiveness at the price of increased policy-management complexity when the access structure becomes large.

Nevertheless, this tradeoff is justified in the present protocol. A simple threshold structure cannot represent the authorization family $\{\{\mathrm{A},\mathrm{B}\},\{\mathrm{A},\mathrm{C}\},\{\mathrm{A},\mathrm{B},\mathrm{C}\}\}$ without also allowing undesired subsets such as $\{\mathrm{B},\mathrm{C}\}$. Tree-based structures are better suited to strictly hierarchical authorization, but are less natural for overlapping coalitions. By contrast, HBAS directly captures fine-grained, overlapping, and message-dependent authorization requirements.

If one only needs a symmetric policy such as t-out-of-n recovery, a threshold-based access structure would indeed be lighter-weight. However, for the present selective-recovery setting, HBAS achieves finer control without increasing the quantum workload of the semi-quantum participants. Designing compressed or hybrid access-control models that preserve this flexibility while reducing policy-management cost for larger networks is an interesting direction for future work.

7.5. Comparison with recent three-party semi-quantum protocols

To position the proposed protocol more clearly with respect to recent related works, we compare it with representative three-party semi-quantum schemes that are closest to the present setting. Since the efficiency definitions used in the literature are not fully uniform, the table below focuses on structural and operational features, while the detailed efficiency and payload discussion is given in the text after the table.

Table 3. Comparison with representative recent three-party semi-quantum protocols.

Protocol	Channel utilization (η)	Pattern	SQ-user operations	Check	Checking states	Fine-grained access	Key advantage
Zhou *et al.*[45]	50%	Symmetric 3-party SQD	Measure and prepare, reflect	2 rounds	Yes	No	Baseline GHZ–SQD
Yang *et al.*[42]	40%	Asymmetric 3-party	Measure and prepare, reorder	2 rounds	Yes	No	Higher reported efficiency
Yang and Liu[49]	13%	3-party SQD	Measure, reflect, prepare	1 round	No	No	Strict SQ compliance
Zhang *et al.*[50]	85.7%	Symmetric 3-party SQD	GHZ-based SQ operations	2 rounds	Yes	No	Dishonest-user robustness
Ours	**$4N$ payload** over N GHZ rounds	Authorization-controlled 3-party SQD	Measure and resend, reflect	2 rounds	Yes	**Yes**	**$4N$ payload + HBAS**

Table 3 shows that recent three-party semi-quantum protocols emphasize different design goals, while their reported channel-utilization values are not always defined under a fully uniform convention. The protocol of Zhou *et al.*[45] is the most direct GHZ-based three-party SQD baseline for the present work, but it does not provide any message-dependent authorization mechanism. Yang *et al.*[42] also consider a GHZ-based three-party semi-quantum setting and report a channel-utilization value of 40%, but their focus is not on fine-grained access control. Yang and Liu[49] emphasize strict compliance with the semi-quantum model by removing probe photons and quantum memory, thereby reducing implementation burden, although at the cost of a lower reported channel-utilization value under their own metric. Zhang *et al.*[50] improve robustness against dishonest-participant attacks and report a markedly higher utilization value, but still do not consider hypergraph-based authorization.

By contrast, the present protocol is designed to combine three properties simultaneously: (i) GHZ-based three-party semi-quantum dialogue, (ii) fine-grained access control via hypergraph-based access structures, and (iii) increased payload at the fully quantum participant through Grover-based 2-bit encoding. Under the same GHZ-round viewpoint used for direct comparison with Zhou *et al.*,[45] the useful message payload increases from $3N$ bits to $4N$ bits over N GHZ rounds. Hence, the relative payload gain is about 33.3%. Therefore,

the main advantage of the proposed protocol is not merely a higher channel-utilization value under one specific convention, but a better combination of payload, authorization flexibility, and semi-quantum implementability.

8. Conclusion

In this work, we have proposed a novel three-party semi-quantum dialogue (3P-SQD) protocol that integrates GHZ-based semi-quantum communication with Grover's algorithm encoding and hypergraph-inspired access control. Compared to previous schemes such as Zhou *et al.*,[45] Ye and Ye,[36] and Shukla *et al.*,[35] the proposed protocol achieves several key improvements.

First, it enhances information throughput by encoding two bits per GHZ round using Grover iterations, while maintaining minimal quantum requirements for semi-quantum participants. In contrast, prior 3P-SQD protocols transmit only one bit per GHZ round from the fully quantum participant, limiting overall communication efficiency. Second, the introduction of hypergraph-based access structures enables fine-grained control over message recovery, ensuring that only authorized subsets of participants can reconstruct specific information. Previous works relied largely on simpler access structures,[15,16] which offer less flexibility in controlling the collaborative information flow. Third, the protocol preserves robust security against standard quantum attacks, including intercept-resend and entanglement-measurement strategies, comparable to existing semi-quantum protocols.[22,45]

In addition to the above theoretical advantages, the protocol also has the potential for practical implementation. First of all, the fully quantum user in our protocol needs to prepare GHZ states as quantum channels. However, existing studies show that GHZ states can be prepared and transmitted with high fidelity in quantum networks. As early as 2010, Neeley *et al.* introduced an experiment for generating GHZ states using superconducting phase qubits in Ref. [51], with an experimental fidelity of approximately 62%. It was reported in Ref. [52] that, in a quantum network where quantum nodes are connected by one-meter-long superconducting coaxial cables, single qubit transmission between superconducting quantum nodes can be achieved with a fidelity of 91.1%, and GHZ states can be deterministically prepared with a fidelity of 65.6%. Therefore, we believe that the preparation of GHZ states by fully quantum users in our protocol is practically feasible, and the transmission of single qubits via quantum channels is robust against noise with low loss. Secondly, the introduction of semi-quantum users turns our protocol into a two-way quantum communication scheme. It has been shown, at least in the theoretical scenario, that two-way channels can improve the noise tolerance of protocols.[27] The channel security detection in our protocol is similar to that in QSDC, which is accomplished through two rounds of probe state detection. In Ref. [53], researchers reported the implementation of a QSDC scheme in a realistic environment with high noise and high loss. The QSDC scheme can effectively send text messages and reasonably sized image and sound files. Therefore, the detection of channel security in our protocol is feasible for implementation. Finally, the difficulty of this protocol lies in the measure and resend operations adopted by semi-quantum users. In a realistic environment, this would be implemented through a photon detector which absorbs the photon and, so, to "resend," Bob would need to prepare a fresh photon, opening the door to multiple attacks.[23,54,55] Meanwhile, some studies have reported semi-quantum communication schemes without resend operations.[30] Our future work will investigate how to abandon the resend operation while still preserving the advantages of the current scheme. Based on the above analysis, we believe that the semi-quantum dialogue protocol proposed in this paper is feasible for implementation.

Acknowledgements

Project supported by the National Natural Science Foundation of China (Grant No. 12201300) and the Nanjing University of Science and Technology Undergraduate Innovation Training Program (Grant No. S202510288017).

References

[1] Bennett C H and Brassard G 2014 *Theoretical Computer Science* **560** 7
[2] Ekert A K 1991 *Phys. Rev. Lett.* **67** 661
[3] Xu F H, Ma X F, Zhang Q, Lo H K and Pan J W 2020 *Rev. Mod. Phys.* **92** 025002
[4] Xu H X, Wang S H, Song Y Q, Zhang P and Wang C L 2025 *Chin. Phys. B* **34** 050310
[5] Zhou C, Wang H T, Lu Y F, Jiang X L, Zhao Y M, Zhou Y, Wang Y, Li J J, Zhou Y Y and Wang X 2024 *Chin. Phys. B* **33** 100302
[6] Cao Y, Yu X, Zhao Y, Zhang C, Zhou X, Zhang J and Wang Q 2025 *Chin. Phys. B* **34** 010310
[7] Deng F G, Long G L and Liu X S 2003 *Phys. Rev. A* **68** 042317
[8] Sheng Y B, Zhou L and Long G L 2022 *Science Bulletin* **67** 367
[9] Lo H K, Curty M and Qi B 2012 *Phys. Rev. Lett.* **108** 130503
[10] Yang L, Wu J W, Lin Z S, Yin L G and Long G L 2020 *Science China Physics, Mechanics & Astronomy* **63** 110311
[11] Pan D, Long G L, Yin L, Sheng Y B, Ruan D, Ng S X, Lu J H and Hanzo L 2024 *IEEE Communications Surveys & Tutorials* **26** 1898
[12] Ying J W, Wang J, Xiao Y, Gu S, Wang X, Zhong W, Du M, Li X, Shen S and Zhang A 2025 *Science China Physics, Mechanics & Astronomy* **68** 240312
[13] Hillery M, Bužek V and Berthiaume A 1999 *Phys. Rev. A* **59** 1829
[14] Ju X X, Zhong W, Sheng Y B and Zhou L 2022 *Chin. Phys. B* **31** 100302
[15] Bai C M, Zhang S J and Liu L 2022 *Quantum Inf. Process.* **21** 119
[16] Bai C M, Shu Y X and Zhang S J 2025 *Scientific Reports* **15** 10819
[17] Zhou X L, Shu Y X, Bai C M and Zhang S J 2025 *Physica Scripta* **100** 105106
[18] Wootters W and Fields B 1989 *Annals of Physics* **191** 363
[19] Bennett C H, Bernstein H, Popescu S and Schumacher B 1996 *Phys. Rev. A* **53** 2046
[20] Gross D, Liu Y, Flammia S T, Becker S and Eisert J 2010 *Phys. Rev. Lett.* **105** 150401
[21] Scarani V, Cerf N J, Dušek M, Lütkenhaus N and Peev M 2009 *Rev. Mod. Phys.* **81** 1301

[22] Boyer M, Kenigsberg D and Mor T 2007 *Quantum key distribution with classical Bob 2007 First International Conference on Quantum, Nano, and Micro Technologies* (ICQNM'07) (IEEE) p. 10
[23] Iqbal H and Krawec W O 2020 *Quantum Inf. Process.* **19** 97
[24] Boyer M, Gelles R, Kenigsberg D and Mor T 2009 *Phys. Rev. A* **79** 032341
[25] Zou X F, Qiu D W, Li L Z, Wu L H and Li L J 2009 *Phys. Rev. A* **79** 052312
[26] Renner R, Gisin N and Kraus B 2005 *Phys. Rev. A* **72** 012332
[27] Amer O and Krawec W O 2019 *Phys. Rev. A* **100** 022319
[28] Krawec W O 2018 *Key-rate bound of a semi-quantum protocol using an entropic uncertainty relation 2018 IEEE International symposium on information theory (ISIT)* (IEEE) pp. 2669–2673
[29] Krawec W O 2017 *Quantum Information and Computation* **17** 0209
[30] Massa F, Yadav P, Moqanaki A, Krawec W O, Mateus P, Paunković N, Souto A and Walther P 2022 *Quantum* **6** 819
[31] Chang L W, Zhang Y Q, Tian X X, Qian Y H and Zheng S H 2020 *Chin. Phys. B* **29** 010304
[32] Shi G F 2021 *Chin. Phys. B* **30** 100303
[33] Zhu P H, Zhong W, Du M M, Li X Y, Zhou L and Sheng Y B 2024 *Chin. Phys. B* **33** 030302
[34] Gu S P, Ying J W, Wang X F, Zhou L and Sheng Y B 2025 *Chin. Phys. B* **34** 110308
[35] Shukla C, Thapliyal K and Pathak A 2017 *Quantum Inf. Process.* **16** 295
[36] Ye T Y and Ye C Q 2018 *International Journal of Theoretical Physics* **57** 1440
[37] Pan H M 2020 *International Journal of Theoretical Physics* **59** 1364
[38] Pan T J, Zhou R G and Zhang X X 2024 *Quantum Inf. Process.* **23** 365
[39] Chen T H 2025 *Future Internet* **17** 263
[40] Zou X F and Qiu D W 2014 *Science China Physics, Mechanics & Astronomy* **57** 1696
[41] Guo H, Li Y X, Wei J H, Tang J and Wang J H 2023 *Chinese Journal of Quantum Electronics* **40** 738
[42] Yang Y F, Duan L Z, Qiu T R, Xie X M and Duan W Y 2022 *Quantum Inf. Process.* **21** 324
[43] Zhao M N, Zhou R G and Feng Y H 2025 *Entropy* **27** 666
[44] Wang H W, Tsai C W, Lin J and Yang C W 2022 *Sensors* **22** 4998
[45] Zhou R G, Zhang X X and Li F X 2021 *Quantum Inf. Process.* **20** 153
[46] Hwang W Y 2003 *Phys. Rev. Lett.* **91** 057901
[47] Lo H K, Ma X and Chen K 2005 *Phys. Rev. Lett.* **94** 230504
[48] Wang X B 2005 *Phys. Rev. Lett.* **94** 230503
[49] Yang C W and Liu P Y 2025 *Quantum Inf. Process.* **24** 207
[50] Zhang L, Liu X, Xin X J, Li C Y and Gong L 2025 *Entropy* **27** 1002
[51] Neeley M, Bialczak R C, Lenander M, Lucero E, Mariantoni M, O'connell A, Sank D, Wang H, Weides M and Wenner J 2010 *Nature* **467** 570
[52] Zhong Y P, Chang H S, Bienfait A, Dumur é, Chou M H, Conner C R, Grebel J, Povey R G, Yan H and Schuster D I 2021 *Nature* **590** 571
[53] 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 and Long G L 2019 *Light: Science & Applications* **8** 22
[54] Tan Y G, Lu H and Cai Q Y 2009 *Phys. Rev. Lett.* **102** 098901
[55] Yang Y G, Sun S J and Zhao Q Q 2015 *Quantum Inf. Process.* **14** 681